1.5.7.13. Secure Fax Contract Reject

Secure Fax Contract Reject Request

BIA Part:

4–byte BIA Identification
4–byte sequence number
encrypted(DUKPT key) Biometric–PIC block:
300–byte authorization biometric
4–12 digit PIC
56–bit response key
fax tracking number
MAC

Terminal Part: (not used)

Secure Fax Contract Reject Response

encrypted(response key):
private code
status code (ok, invalid individual)
MAC

The DPC uses the biometric–PIC to identify the individual making the Contract Reject request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status. Otherwise, the DPC updates the Recipient record's contract status field to "rejected" and generates a Status Notice to the fax's sender (see Fax Data, above).

1.5.7.14. Secure Fax Organization Change

Secure Fax Organization Change (Secure Fax message)
sender name, company, title, and fax number
list of organizational changes

Organization changes are submitted to the DPC via a secure fax message. A customer support engineer enters the changes requested in the fax

message, verifying that the individual submitting the request is allowed to register individuals for that particular company. Since the fax is a secure fax, the sender's identity has already been ascertained, as has his title.

1.5.7.15. Electronic Document Submit

Electronic Document Submit Request

BIA Part:

- 4–byte BIA Identification
- 4–byte sequence number
- *encrypted(DUKPT key) Biometric–PIC block:*
  - 300–byte authorization biometric
  - 4–12 digit PIC
  - 56–bit response key
  - 56–bit message key
- recipient list
- MAC

Terminal Part: (not used)

Electronic Document Submit Response

- *encrypted(response key):*
  - private code text
- tracking number
- status code (ok, invalid recipient)
- MAC

When the DPC receives an Electronic Document Submit request, it identifies the individual by following the individual identification procedure.

The DPC then creates an EDD Document record and assigns it a unique tracking number. The DPC initializes the record's sender identification code to be the biometric identification code of the identified individual and the message key to be the message key in the request.

Next, the DPC searches the Individual Biometric Database for each recipient and creates an EDD Recipient record for each one. Each record is initialized with the tracking number, the recipient's biometric identification

code, and a delivery status of "incomplete". If any of the recipients cannot be found, the DPC replies with an "invalid recipient" status.

1.5.7.16. Electronic Document Data

Electronic Document Data Request

BIA Part: (not used)

Terminal Part:

tracking number
command (either abort or data)
[optional message offset]
completion indication
encrypted(message key):
message body

Electronic Document Data Response

status (incomplete, ok)

The Electronic Document Data request allows an individual to send the document text (in one or more parts) to the EDD for delivery to the recipient(s). This request does not involve any biometric identification, instead, it relies upon the secret message key to securely transmit the document text.

The request text is assumed to be encrypted by the message key stored in the EDD document record and is appended to the document text already stored in the record.

When the EDD receives a packet with the "document complete" indicator, it knows that the sender has finished transmitting the document. The EDD now sends an Arrival Notice to all recipients of the document via Internet electronic mail informing them that they have a document waiting.

The Arrival Notice is as follows:

Electronic Document Arrival Notice (Internet E-mail message)
sender name, company, title, and e-mail address
tracking number
instructions on how to receive the electronic document

The EDD also updates the status of the EDD recipient record to "notified". When all recipients have either retrieved or rejected the electronic document, the DPC sends a Status Notice via Internet electronic mail to the document originator.

The Status Notice is as follows:

Electronic Document Status Notice (Internet E–mail message)
- sender name, company, title, and e–mail address
- tracking number
- list of recipients showing for each
  - name, company, title, e–mail address
  - delivery date and status

The DPC finds each individual's company and title information in the EDD Organization table.

1.5.7.17. Electronic Document Retrieve

Electronic Document Retrieve Request

BIA Part:
- 4–byte BIA Identification
- 4–byte sequence number
- *encrypted(DUKPT key) Biometric–PIC block:*
  - 300–byte authorization biometric
  - 4–12 digit PIC
  - 56–bit response key
- tracking number
- MAC

Terminal Part: (not used)

Electronic Document Retrieve Response

encrypted(response key):
private code
56–bit message key
status (incomplete, ok, invalid recipient)
MAC
encrypted(message key):
document text

The DPC uses the biometric–PIC to identify the individual making the electronic document retrieve request by following the individual identification procedure.

The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification.

If the record cannot be found, then the request fails with an "invalid recipient" status. Otherwise, the DPC sends the document's message key and the document (still encrypted by the message key) to the requester.

The EDD then updates the status of the EDD recipient record to "retrieved". When all recipients have either retrieved or rejected the document, the DPC sends a Status Notice via Internet electronic mail to the document originator (see Electronic Document Data, above) and then schedules to remove the Document and Recipient records (see Secure Fax Retrieve, above)

1.5.7.18. Electronic Document Reject

Electronic Document Reject Request

BIA Part:
4–byte BIA Identification
4–byte sequence number
encrypted(DUKPT key) Biometric–PIC block:
300–byte authorization biometric
4–12 digit PIC
56–bit response key
message tracking number
MAC
Terminal Part: (not used)

Electronic Document Reject Response

encrypted(response key):

private code

status code (ok, invalid recipient)

MAC

The DPC uses the biometric–PIC to identify the individual making the electronic document reject request. The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification. If the record cannot be found, then the request fails with an "invalid recipient" status.

The EDD updates the status of the EDD recipient record to "rejected". The DPC then follows the same notification and deletion procedure as described in Electronic Document Retrieve, above.

1.5.7.19. Electronic Document Archive

Electronic Document Archive Request

BIA Part:

4–byte BIA Identification

4–byte sequence number

encrypted(DUKPT key) Biometric–PIC block:

300–byte authorization biometric

4–12 digit PIC

56–bit response key

tracking number

MAC

Terminal Part: (not used)

Electronic Document Archive Response

encrypted(response key):

private code

status code (ok, invalid individual)

MAC

The DPC uses the biometric–PIC to identify the individual making the electronic document archive request. The DPC finds the EDD Recipient record keyed by the request's tracking number and the individual's biometric Identification. If the record cannot be found and the individual is not the sender or one of the recipients, then the request fails with an "invalid individual" status. Otherwise, the DPC copies the Document and Recipient records into the EDD archive database. Any subsequent changes to these records are also copied to the archived versions.

1.5.7.20. Electronic Document Archive Retrieve

Electronic Document Archive Retrieve Request

BIA Part:

4–byte BIA Identification

4–byte sequence number

encrypted(DUKPT key) Biometric–PIC block:

300–byte authorization biometric

4–12 digit PIC

56–bit response key

optional title index code, sending fax number, and extension

tracking number

MAC

Terminal Part: (not used)

Electronic Document Archive Retrieve Response

encrypted(response key):

private code

status code (ok, invalid individual)

MAC

The DPC can receive an Electronic Document Archive Retrieve request from either a Secure Fax Terminal or a Certified Email Terminal. The DPC uses the individual identification procedure to determine the individual submitting the archive retrieve request. The individual must be either the sender or one of the recipients or else the DPC denies the request by setting the status code to "invalid individual". However, if the archived document was

a fax sent using a corporate title, the DPC allows additional individuals whose titles are higher in the corporate hierarchy to retrieve the archived document as well.

The EDD maintains an archive database, indexed by the document's original tracking number, stored on off-line media such as CD-ROMs and tape that can take considerable time to search for the archived document. As a result, the DPC does not return the archived document immediately, but instead informs the requesting individual that the DPC has begun the search. At a later date when the DPC finishes the search, it notifies the requester that the archived document is ready to be retrieved through the standard document arrival notification mechanisms -- either via fax or email, depending on the format of the original document.

The DPC creates an EDD archive request record to store information about the requester so that when the search completes, the DPC remembers to whom to send the document.

1.5.7.21. Electronic Signature

Electronic Signature Request

BIA Part:

- 4-byte BIA Identification
- 4-byte sequence number
- *encrypted(DUKPT key) Biometric-PIC block:*
  - 300-byte authorization biometric
  - 4-12 digit PIC
  - 56-bit response key
- document name
- document MD5 calculation
- MAC

Terminal Part: (not used)

Electronic Signature Response

- *encrypted(response key):*
  - private code text
- signature string
- MAC

To process the electronic signature request, the DPC first performs a biometric identification using the biometric–PIC. Then, the DPC creates an ESD record, assigns it a unique signature identification code, and sets the record's signature field to the electronic signature in the request. The DPC then returns a signature string that can be submitted for later verification:

"<Dr. Bunsen Honeydew> <Explosions in the Laboratory> 5/17/95 13:00 PST 950517000102"

1.5.7.22. Electronic Signature Verify

Electronic Signature Verification Request

BIA Part:

4–byte BIA Identification
4–byte sequence number
encrypted(DUKPT key) Biometric–PIC block:
300–byte authorization biometric
4–12 digit PIC
56–bit response key
signature string
MAC

Terminal Part: (not used)

Electronic Signature Verification Response

encrypted(response key):
private code text
signature string
status (verified, failed)
MAC

The DPC performs a biometric identification, extracts the signature tracking code from the signature string, retrieves the indicated ESD record, and verifies that it matches the signature string. The DPC returns the private code and the outcome of the signature comparison.

1.5.7.23 Network Credential

Network Credential Request

BIA Part:

- 4–byte BIA Identification
- 4–byte sequence number
- *encrypted(DUKPT key) Biometric–PIC block:*
  - 300–byte authorization biometric
  - 4–12 digit PIC
  - 56–bit response key
- account index
- bank code
- bank hostname
- terminal.port and bank.port (TCP/IP addresses)
- MAC

Network Credential Response

- *encrypted(response key):*
  - private code
- *signed(DPC's private key):*
  - credential(time, acct, terminal.port, bank.port)
- bank's public key
- status code (ok, failed)
- MAC

The DPC identifies the individual using the request's biometric–PIC and retrieves the individual's asset account stored at the specified index. If the account index is the emergency account, then the network credential response status code is set to "failed" and no credential is generated.

The DPC constructs the credential using the current time, the retrieved asset account, and the TCP/IP addresses of the terminal and the bank. The DPC then uses public key encryption to sign the credential with its private key.

The response also includes the bank's public key, which the DPC retrieves from the Remote Merchant Database.

1.5.8. Customer Support and System Administration Messages

The DPC handles additional message types classified as internal messages. The DPC generally does not accept these messages from non–DPC systems. The messages are database vendor specific. However, the internal network uses DES–encrypted packets to provide additional security.

The Customer Service and System Administration tasks are implemented using the database vendor's query language and application development tools.

1.5.8.1. Customer Service tasks:

- IBD: find, activate, deactivate, remove, correct records.
- AID: add or remove authorized individuals.
- AOD: find, add, remove, correct records.
- VAD: find, activate, deactivate, remove, correct records.
- RMD: find, add, remove, correct records.
- PFD: add, remove, correct records.

1.5.8.2. System Administration tasks:

- Run prior fraud checks.
- Modify the Valid Site List.
- Summarize log information (warnings, errors, etc.).
- Modify the PIC Group List.
- Performance monitoring.
- Run backups.
- Crash recovery procedures.
- Time synchronization for the DPC sites.
- Change the primary registration site.
- Change the secret DES encryption key.
- Clean up old document tracking numbers.
- Generate a list of BIA hardware identification code, MAC encryption key, and DUKPT Base Key triples. Store on an encrypted floppy for the Key Loading Device.

1.5.9. Firewall Machine

1.5.9.1. Purpose

The FW Machines provide a first line of defense against network viruses and computer hackers. All communication links into or out of the DPC site first pass through a secure FW Machine.

1.5.9.2. Usage

The FW Machine, an internet–localnet router, only handles messages destined for the GM Machines.

BIA–equipped terminals send packets to a single DPC site via modem, X.25, or other communication medium. The DPC relies on a third party to supply the modem banks required to handle the volume of calls and feed the data onto the DPC backbone.

For DPC to DPC communication, primarily for distributed transactions and sequence number updates, the FW Machines send out double–length DES encrypted packets. The DPC LAN component handles the encryption and decryption: the FWs do not have the ability to decrypt the packets.

1.5.9.3. Security

A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

The FW disallows any transmissions from the internal network to the rest of the Internet.

1.5.9.4. Message Bandwidth

A transaction authorization request requires about 400 bytes and registration packets require about 2 KB. To handle 1000 transaction authorizations per second and 1 registration packet per second, the FW

Machines are able to process about 400 KB per second (all known in the industry).

Each DPC site requires an aggregate bandwidth of nearly three T1 connections to the third party modem bank and the other DPC sites.

1.5.10. Gateway Machine

1.5.10.1. Purpose

The GM Machine (GM), through the FW Machines, link the outside world (BIA-equipped terminals and other DPCs) to the internal components of the DPC. The DPC has multiple GMs, typically two.

1.5.10.2. Usage

The GM supervises the processing of each BIA request, communicates with the various DPC components as necessary, and sends the encrypted results of the request back to the sender. The software performing this task is called the Message Processing Module.

The GM logs all requests it receives and any warnings from components it communicates with. For example, the GM logs any emergency account accesses, sequence number gaps, and invalid packets.

Processing a request may require the GM to inform GMs at all other DPCs of a change in the DPC databases. When this happens, the GM runs a distributed transaction to update the remote databases.

Distributed transactions fall into two categories: synchronous and asynchronous. Synchronous distributed transactions require the GM to wait for the distributed transaction to commit before continuing to process the packet. Asynchronous distributed transactions do not require the GM to wait for the commit, and allow it to finish processing the request regardless of whether the distributed transaction commits or not. Asynchronous distributed transactions are only used to update data for which database consistency is not an absolute requirement: sequence numbers and biometric checksum recordings may be performed asynchronously, whereas creating database records, such as Individual Biometric records, may not.

When executing a synchronous distributed transaction, the requesting GM only considers the entire transaction successful if all sites can successfully commit the transaction locally. Otherwise, the GMs back out the changes locally and reject the request due to a transaction error.

The list of valid DPC sites is normally all of the sites. In the case of an extreme site failure, however, a system administrator may manually remove that site from the valid site list. The most likely cause of distributed transaction failures, however, are temporary network failures that are unrelated to any DPC equipment. Requests that require a synchronous distributed transaction cannot be performed until network connectivity is restored or the site is removed from the valid site list. Before a site can be added back to the valid site list, the system administrator brings the site's databases up to date with those of a currently active site.

1.5.10.3. Software Components

Each GM runs the following software components locally for performance reasons:

Message Processing Module
Message Authentication Code Module
Message Decrypt Module
Individual Biometric Database Machine List

1.5.10.4. Message Bandwidth

The message bandwidth required by the GMs is similar to that required by the FW Machines. A FDDI network interface provides 100 MBits per second and easily covers any bandwidth requirements.

1.5.11 DPC LAN

1.5.11.1 Purpose

The DPC Local Area Network (LAN) links the machines of the DPC sites together using a fiber optic token ring. The fiber optic token ring provides both high bandwidth and good physical security.

1.5.11.2 Security

The network interfaces used by the machines on the DPC LAN include encryption hardware to make tapping or intercepting packets useless without the encryption key. The encryption key is the same for all machines on the LAN and is stored in the encryption hardware.

A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

1.5.12 Message Processing Module

1.5.12.1 Purpose

The Message Processing Module (MPM) handles the processing for a request packet. It communicates with other components of the DPC as necessary to perform its tasks. The presence of an MPM on a machine brands it as a GM.

1.5.12.2 Usage

The MPM maintains a request context for each request it is currently processing. The request context includes the information necessary to maintain the network connection to the terminal making the request, the BIA device information, the response key, and the response packet.

1.5.13. Message Authentication Code Module

1.5.13.1. Purpose

The Message Authentication Code Module's (MACM) tasks are to validate the Message Authentication Code on inbound packets and to add a Message Authentication Code to outbound packets.

1.5.13.2. Usage

The MACM maintains an in–memory hash table of 112–bit MAC encryption keys keyed by BIA hardware identification code.

When the MACM receives a request from the GM to validate a packet's MAC, it first looks up the packet's hardware identification code in the hash table. If no entry exists, then the MACM replies to the GM with an "invalid hardware identification code" error.

Otherwise, the MACM performs a MAC check on the BIA message part of the packet using the 112–bit MAC encryption key. If the MAC check fails, then the MACM replies to the GM with an "invalid MAC" error. Otherwise, the MACM replies with a "valid MAC" message.

If the packet contains a merchant code, the MACM also checks the merchant code against the owner identification code in the hash table. If the codes don't match, then the MACM replies with an "invalid owner" error.

When the MACM receives a request from the GM to generate a MAC for a packet, it looks up the MAC encryption key using the packet's hardware identification code. With the MAC encryption key, the MACM generates a MAC and adds it to the packet. If the MACM cannot find the hardware identification code in its hash table, it replies with an invalid hardware identification code error instead.

1.5.13.3. Database Schema

The MACM hash table entry contains:

```
MACM Entry:
    hardwareId = int4
    ownerId = int4
    macEncryptionKey = int16
```

The table is hashed by hardware identification code.

1.5.13.4. Database Size

Assuming 5 million BIA–equipped devices in service, the hash table requires about 120 MB of storage. For performance reasons, this hash table is cached completely in memory.

1.5.13.5. Dependencies

The MACM only contains records referencing active BIA hardware identification codes and active apparatus owners. Whenever an apparatus or apparatus owner is suspended or deleted from the system, the MACM removes any entries that reference the identification code. When an apparatus is activated, the MACM then adds an entry for it.

The MACM also caches the MAC encryption key from the Valid Apparatus Database. Since the system does not allow the encryption key of an BIA to be changed, the MACM does not need to worry about receiving encryption key updates.

1.5.14. Message Decrypt Module

1.5.14.1. Purpose

The Message Decrypt Module's (MDM) task is to reconstruct the DUKPT transaction key and with it decrypt the biometric– PIC block of the packet. It maintains a list of the DUKPT Base Keys that are required to generate the transaction key.

1.5.14.2. Usage

The MDM constructs the DUKPT transaction key using the packet's sequence number as the DUKPT transaction counter, the upper 22 bits of the BIA hardware identification code as the DUKPT tamper resistant security module (or "TRSM") Identification, and the low 10 bits of the BIA hardware identification code as the DUKPT Key Set Identification.

The DUKPT standard specifies how the transaction key is generated. The Key Set Identification is used to look up a Base Key from the

Base Key List. The Base Key is used to transform the TRSM Identification into the initial key via a DES encrypt/decrypt/encrypt cycle. The transaction counter is then applied to the initial key as a series of DES encrypt/decrypt/encrypt cycles to generate the transaction key.

For additional security, two Base Key Lists are maintained, one for low security BIA devices and one for high security devices. The MDM chooses which Base Key List to use depending on the security level of the device.

1.5.14.3. Database Schema

The MDM Base Key List entry contains:

MDM Entry:

baseKey = int16

The Base Key List is indexed by Key Set Identification.

1.5.14.4. Database Size

The MDM maintains an in–memory list of the DUKPT Base Keys. Each key requires 112–bits. The MDM maintains two sets of 1024 keys requiring 32 KB total.

1.5.14.5. Dependencies

The MDM has no direct dependencies on any other DPC component.

1.5.15. PIC Group List

1.5.15.1. Purpose

The PIC Group List (PGL), in conjunction with the Individual Biometric Database Machine List, defines the configuration of the IBD machines. The PGL stores a list of the PIC groups in the system which is used to simplify the management of the PICs. A PIC group is a set of consecutive PIC codes. A PGL exists on each GM Machine (GM).

1.5.15.2. Usage

The PGL, when given a PIC code, searches through its list of PIC groups for the group containing the PIC code. The PGL maintains the list of groups in order and uses a binary search to quickly find the correct group.

The initial configuration for the PGL is one giant PIC group containing all possible PICs. After a threshold number of PICs are assigned, the giant PIC group is split in two. Thereafter, this process is applied to all succeeding PIC groups.

When a PIC group splits, the PGL assigns a new main and backup IBD machine based on available storage on a first–come–first serve basis. The PGL coordinates with the IBD machines to first copy the affected records from the old main and backup machines to the new ones, update the IML record, and last remove the old main and backup copies. Splitting a PIC group is an involved task. The PGL batches split requests to be run when the DPC is lightly loaded, for instance, at night.

The system administrator may also change the main and backup IBD machines for a given PIC group if the machines' free storage falls below a level required for handling the expected amount of new registrations.

1.5.15.3. Database Schema

The schema for the PIC Group records are:

```
PICGroup:
        lowPin = int8
        highPin = int8
        used = int4
```

Each PIC group is identified by a unique identifier. For convenience the PIC group identification code is the lowPin code for the group, however the system does not otherwise rely upon this fact.

The PGL is keyed by the lowPin field.

1.5.15.4. Database Size

The PGL is expected to contain about 3000 groups (each PIC group contains about 1000 active PICs, but may span millions of actual PICs). The entire PGL requires about 72 KB of storage and is cached completely in memory.

1.5.15.5. Dependencies

When PIC groups are added, merged, or split up, the PGL is responsible for informing the IBD Machine List of the changes and for directing the movement of IBD records from one IBD machine to another.

1.5.16. Individual Biometric Database Machine List

1.5.16.1. Purpose

The IBD Machine List (IML), in conjunction with the PIC Group List, codifies the configuration of the IBD machines. The IML maps a PIC code to the main and backup IBD machines storing IBD records for the PIC. The IML is actually keyed by PIC Group (a set of consecutive PIC codes) rather than by individual PICs because this greatly reduces the memory required to store the list. An IML exists on each GM Machine (GM).

1.5.16.2. Usage

When a GM processes a request that requires a biometric identification, the GM finds the IML record keyed by the biometric's PIC group. The GM then knows the main and backup IBD machines to use for the biometric identification.

1.5.16.3. Database Schema

The schema for the IML list entries are:

```
MachinePair:
        pinGroup = int8
        main = int2,
        backup = int2
```

The IML is keyed by pinGroup.

1.5.16.4. Database Size

The IML is expected to contain about 3000 entries (the number of PIC Groups). Each MachinePair record is 12 bytes requiring about 36 KB of storage and is cached completely in memory.

1.5.16.5. Dependencies

Any changes in the configuration of the IBD machines are be reflected in the IML. In addition, the IML uses PIC groups for its keys so when the PIC Group List gets modified, the IML are also updated.

1.5.17. Sequence Number Module

1.5.17.1. Purpose

The Sequence Number Module's (SNM) primary function is to prevent replay attacks by validating packet sequence numbers. Its secondary task is to minimize the effects of a resubmission attack by informing other SNMs in remote DPC sites of sequence number updates and to periodically update the sequence numbers in the Valid Apparatus Database.

The SNM maintains an in-memory hash table of sequence numbers keyed by BIA hardware identification code codes to allow quick validation of packet sequence numbers.

1.5.17.2. Usage

When the SNM receives a validate request from the GM for a given hardware identification code and sequence number, it looks up the hardware identification code in the hash table. If no entry exists, then the SNM replies to the GM with an "invalid hardware identification code" error.

Otherwise, the SNM checks the given sequence number against the sequence number stored in the hash table entry. If the sequence number is less than or equal to the stored sequence number, the SNM replies with an "invalid sequence number" error. Otherwise, the SNM sets the sequence number in the hash table entry to the given sequence number and replies with a "valid sequence number" message.

From time to time, the SNM may observe a sequence number gap. A sequence number gap occurs when the SNM receives a sequence number that is more than one greater than the sequence number stored in the hash table entry. In other words, a sequence number was skipped. When the SNM discovers a sequence number gap, it replies with a "sequence number gap" message to the GM instead of a "valid sequence number" message. The GM treats the packet as valid, but it also logs a "sequence number gap" warning.

Sequence number gaps usually occur when network connectivity is lost: packets are dropped or can't be sent until the network is restored to working order. However, sequence number gaps occur for fraudulent reasons as well: malicious parties could intercept packets preventing them from arriving at the DPC or they could even attempt to counterfeit packets (with a large sequence number so that it isn't immediately rejected).

The SNM's secondary function is to inform other DPCs of the updated sequence numbers. Quickly updating sequence numbers at all DPC sites thwarts resubmission attacks wherein a malicious entity monitors packets whose destination is for one DPC site and immediately sends a copy to a different DPC site in the hope of exploiting the transmission delay of sequence number updates from one DPC site to another resulting in both sites accepting the packet as valid, when only the first site should accept the packet.

The SNMs send update messages to each other whenever they receive a valid sequence number. If an SNM receives an update message for a sequence number that is less than or equal to the sequence number currently

stored in its hash table, that SNM logs a sequence number resubmission warning. All resubmission attacks are detected in this manner.

A simpler way to thwart resubmission attacks completely, is to have only one SNM validate packets. Under this scheme, there is no update transmission delay window to exploit with a resubmission attack. Alternately, multiple SNMs can be active at the same time provided none of them handle sequence number validation for the same BIA–equipped device.

1.5.17.3. Sequence Number Maintenance

When the SNM boots up, it loads the sequence number hash table from the sequence numbers for active BIA stored in the VAD.

Once per day, the SNM downloads the current sequence numbers to the local Valid Apparatus Database (VAD).

The VAD is responsible for sending add–entry and remove– entry messages to the SNMs for any BIA–equipped devices that are activated or deactivated to keep the SNM hash table up–to–date.

1.5.17.4. Database Schema

The SNM hash table entry contains:

SNM Entry:
hardwareId = int4
sequenceNumber = int4

The hash table is keyed by hardwareId.

1.5.17.5. Database Size

Assuming about 5 million BIA–equipped devices in service requires the hash table to be about 40 MB.

1.5.17.6. Dependencies

The SNM depends on the Valid Apparatus Database. When an apparatus is suspended or removed from the database, the SNM removes the corresponding entry. When an apparatus is activated, the SNM creates an entry for it.

1.5.17.7. Message Bandwidth

The SNMs require a transmission bandwidth of about 8 KB per second to handle 1000 update sequence number messages per second. The update sequence number messages is buffered and sent out once per second to minimize the number of actual messages sent.

1.5.18. Apparatus Owner Database

1.5.18.1. Purpose

The Apparatus Owner Database (AOD) stores information on individuals or organizations that own one or more BIA–equipped devices. This information is used to double check that the BIA devices are used only by their rightful owners, to provide asset account information for financial credit and debit transactions, and to allow identification of all BIAs owned by a specific individual or organization.

1.5.18.2. Usage

Each AOD record includes an asset account to credit or debit the owner when the DPC processes a financial transaction submitted by one of the owner's BIA–equipped devices. For instance, transactions submitted from BIA attached to a retail point of sale terminal involves credits to the asset account, while certified electronic mail transmissions results in debits to the asset account.

1.5.18.3. Database Schema

The schema for the Apparatus Owner record is:

ApparatusOwner:

ownerId = int4
name = char50
address = char50
zipCode = char9
assetAccount = char16
status = int1

The status field is one of:

0: suspended
1: active

The Apparatus Owner Database is keyed by ownerId.

1.5.18.4. Database size

The AOD is expected to store about 2 million Apparatus Owner records. Each entry is 130 bytes requiring about 260 MB of storage. The AOD is stored as a hashed file keyed by owner identification code. A copy of the AOD is stored on each GM.

1.5.18.5. Dependencies

When entries are removed or suspended from the AOD, any Valid Apparatus Database records that reference those apparatus owners are marked as suspended. In addition, the MAC Module and the Sequence Number Module remove their entries for the suspended apparatuses.

1.5.19. Valid Apparatus Database

1.5.19.1. Purpose

The Valid Apparatus Database (VAD) is a collection of records representing all of the BIAs that have been manufactured to date. The VAD

record contains the Message Authentication Code encryption key for each BIA, as well as an indication of whether an BIA is active, awaiting shipment, or marked as destroyed. In order for a message from an BIA to be decrypted, the BIA must exist and have an active record in the VAD.

1.5.19.2. Usage

When manufactured, each BIA has a unique public identification code and a unique MAC encryption key, both of which are entered into the VAD record prior to BIA deployment.

When an BIA is first constructed, it is given a unique hardware identification code. When an BIA is placed in service, its hardware identification code is registered with the system. First, the owner or responsible party of the BIA is entered into the Apparatus Owner Database (AOD). Then, the VAD record is pointed to the AOD record, and the BIA is then set active. Requests from that BIA are accepted by the DPC.

When an BIA is removed from service, it is marked as inactive, and the link to the AOD record is broken. No communications from that BIA are accepted.

Each BIA type and model has a security level assigned to it that indicates its level of physical security. When the DPC processes requests from that BIA, it uses the BIA's security level to gauge what kind of actions are allowed. The DPC also provides the security level to external financial transaction authorization services.

For example, a financial transaction authorization service can decide to deny any request for over $300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.

The security levels and the actions that they allow are determined operationally. Basically, the cost to defraud the system must be higher than the potential gain, so the security level is related to the cost to compromise the device.

1.5.19.3. Database Schema

The schema for the Valid Apparatus record is:

Valid Apparatus:

- hardwareId = int4
- macEncryptionKey = int16
- ownerId = int8
- mfgDate = time
- inServiceDate = time
- securityLevel = int2
- status = int1
- type = int1
- use = int1

Possible values for the status field are:

- 0: suspended
- 1: active
- 2: destroyed

Possible values for the type field are (one for each type of terminal):

- 0: ATM
- 1: BRT
- 2: CET
- 3: CPT
- 4: CST
- 5: EST
- 6: IPT
- 7: IT
- 8: ITT
- 9: PPT
- 10: RPT
- 11: SFT

Possible values for the use field are:

0: retail

1: personal

2: issuer

3: remote

The Valid Apparatus Database is keyed by hardware identification code.

1.5.19.4. Database Size

The VAD handles about 5 million retail, issuer, and remote Valid Apparatus entries. Each entry is 51 bytes requiring about 255 MB total. The VAD is stored as a hashed file keyed by hardware identification code. A copy of the VAD is stored on each GM.

The number of personal Valid Apparatus entries number in the range of 30 million requiring another 1.5 GB of storage.

1.5.19.5. Dependencies

When a VAD record changes status, the MAC Modules and Sequence Number Modules are informed of its change in status. For instance, when an apparatus becomes active, the MACP and SNM adds an entry for the newly active apparatus. When an apparatus becomes inactive, the MACP and SNM remove their entry for the apparatus.

1.5.20. Individual Biometric Database

1.5.20.1. Purpose

Individual Biometric Database (IBD) records store information on individuals, including their primary and secondary biometrics, PIC code, list of financial asset accounts, private code, emergency account, address, and phone number. The individual may optionally include their SSN and electronic mail address. This information is necessary for identifying an individual either by biometric or personal information, for accessing account information, or for

providing an address or phone number to remote merchants for additional verification.

1.5.20.2. Usage

Individuals are added to the system during the individual enrollment process at registered Biometric Registration Terminals located in retail banking establishments worldwide, or in local system offices. During enrollment, individuals select their personal identification numbers, and add financial asset accounts to their biometric and PIC combination.

Individuals may be removed from the database due to fraudulent activity reported by any issuing member. If this occurs, the individual's account information is moved from the IBD to the Prior Fraud Database (PFD) by an authorized internal systems representative. The biometric Ids for records in the PFD may not be used for records in the IBD.

The IBD exists on multiple machines, each of which is responsible for a subset of the IBD records with a copy of each record stored on two different machines, both for redundancy and for load-sharing. The IBD Machine List, stored on the GM, maintains which machines hold which PICs.

1.5.20.3. Database Schema

The schema for the Individual Biometric record is:

```
IndividualBiometric:
        primaryBiometric = biometric
        secondaryBiometric = biometric
        biometricId = int4
        PIC = char10
        phoneNumber = char12
        lastName = char24
        firstName = char24
        middleInitial = char2
        SSN = char9
        privateCode = char40
        address = char50
        zipCode = char9
```

publicKey = char64
checksums = int4[10]
accountLinks = char30[10]
emergencyIndex = char1
emergencyLink = char1
privs = char10
enroller = int8
emergencyUseCount = int4
status = int1

The status field is one of:

0: suspended
1: active
2: priorFraud

The IBD is keyed by PIC.

1.5.20.4. Database Indexes

Each IBD machine has additional indexes on the individual's Social Security Number, biometric identification code, last name, first name, and phone number to facilitate access to the IBD database.

1.5.20.5. Database Size

Each IBD machine has 40 GB of secondary storage provided by one or more RAID devices. Each IBD record is 2658 bytes (assuming the biometrics are 1K apiece) allowing up to 15 million records per machine. The IBD records are stored using a (perhaps clustered) secondary index on the PIC. The index is stored in memory and requires no more than 64 MB (a 64 MB index handles about 16 million entries). To store records for 300 million individuals, the DPC needs at least 40 IBD machines: 20 IBD machines for main storage and another 20 for backup. The number of IBD machines is easily scaled up or down depending on the number of registered individuals.

1.5.20.6. Dependencies

The IBD machines, PIC Group List, and the IBD Machine List remain up–to–date in terms of which PICs are on which machine. When a PIC group is reconfigured or main and backup machines for PIC groups are changed, the IBD machines update their databases and indexes appropriately.

1.5.21. Authorized Individual Database

1.5.21.1. Purpose

For each issuer or personal BIA–equipped device, the Authorized Individual Database (AID) maintains a list of individuals who are authorized, by the owner of the device, to use it.

The AID exists for two reasons. The first is that it provides restricted access to a terminal. For example, the Issuer Terminal can only be used by an authorized bank representative. The second reason for the AID is to prevent criminals from secretly replacing the BIA in a retail point of sale terminal with that of a personal BIA from a phone Terminal and thus routing all purchases to a remote merchant account set up by the criminals.

1.5.21.2. Database Schema

The schema for the Authorized Individual record is:

Authorized Individual:
hardwareId = int4
biometricId = int4

The hardwareId refers to a record in the Valid Apparatus Database and the biometricId refers to a record in the Individual Biometric Database. Whenever the DPC needs to check whether an individual is authorized to use a personal or issuer BIA device, the DPC checks for the existence of an Authorized Individual record with the correct hardwareId and biometricId.

Personal BIA devices are identified by a use field set to 1 (personal) in the Valid Apparatus Database. Issuer BIA devices are identified by a use field set to 2 (issuer) in the Valid Apparatus Database.

1.5.21.3. Database Size

Assuming each issuer terminal has 10 individuals authorized to use it and an each personal device has 2 additional authorized individuals with 1,000,000 personal devices in the server, the AID stores about:

$$10 * 100{,}000 + 2 * 1{,}000{,}000 = 3{,}000{,}000 \text{ entries}$$

The entire database requires about 24 MB of storage.

1.5.21.4. Dependencies

When Authorized Owner Database records or Valid Apparatus Database records are removed, all Authorized Individual records referencing them are removed.

1.5.22. Prior Fraud Database

1.5.22.1. Purpose

The Prior Fraud Database (PFD) is a collection of records representing individuals who have defrauded member issuers at some point in the past. The PFD also runs background transactions during periods of low system activity to weed out individuals in the IBD who have matching records in the PFD.

The system does not automatically put individuals in the PFD, unless it detects that they are attempting to register again. Placing an individual in the PFD is a sensitive policy matter which is outside the scope of this document.

1.5.22.2. Usage

Before a new IBD record is marked as active, the individual's primary and secondary biometrics are checked against each and every biometric in the PFD using the same biometric comparison techniques as those

used in the individual identification procedure.. If a match is found for the new IBD record, the IBD record's status is set to "prior fraud". If the prior fraud check was executed as part of a registration request, the GM logs a "registering individual with prior fraud" warning.

It is assumed that the PFD will remain relatively small. The cost to run the PFD is expensive, as it is an involuntary biometric search, so it is important to add only those individuals to the PFD who have imposed a significant cost to the system.

1.5.22.3. Database Schema

The schema for the Prior Fraud record is:

```
Prior Fraud:
        primaryBiometric = biometric
        secondaryBiometric = biometric
        biometricId = int4
        PIC = char10
        phoneNumber = char12
        lastName = char24
        firstName = char24
        middleInitial = char2
        SSN = char9
        privateSignal = char40
        address = char50
        zipCode = char9
        publicKey = char64
        checksums = int4[10]
        accountLinks = char30[10]
        emergencyIndex = char1
        emergencyLink = char1
        privs = char10
        enroller = int8
        emergencyUseCount = int4
        status = int1
```

The status field is one of:

0: suspended

1: active

2: prior fraud

The PFD is keyed by biometric identification code.

1.5.22.4. Database Size

The PFD record is the same as the IBD record. Fortunately, the DPC needs to store a lot less of them so only two database machines are required to store the entire database, of which one is the backup.

1.5.22.5. Dependencies

The PFD does not have any direct dependencies on any other DPC component.

1.5.23. Issuer Database

1.5.23.1. Purpose

The Issuer Database (ID) stores information on banks and other financial institutions that allow their asset accounts to be accessed through the system. The issuing institutions are the only entities that can add or remove their asset account numbers to a given individual's IBD record.

1.5.23.2. Usage

The DPC uses the ID to validate requests from Issuer Terminals by searching the ID for a record containing the Issuer Terminal's issuer code. The owner Identification stored in the record must match up with the owner stored in the Valid Apparatus Database for the BIA stored in the Issuer Terminal.

The schema for the Issuer record is:

Issuer Record:

issuerCode = int6
ownerId = int4
name = char50
phoneNumber = char12
address = char50
zipCode = char9

The Issuer Database is keyed by issuerCode.

1.5.23.3. Database Size

The Issuer Database handles about 100,000 entries. Each entry is 127 bytes requiring less than 2 MB. A copy of the ID is stored on each GM.

1.5.23.4. Dependencies

The Issuer Database does not have any direct dependencies on any other DPC component.

1.5.24. Electronic Document Database

1.5.24.1. Purpose

The Electronic Document Database (EDD) stores and tracks electronic documents such as fax images and electronic mail messages destined for specified individuals. It also maintains corporate organizational charts to provide the official titles of both sender and receiver. The EDD also archives the documents at the sender or receiver's request and provides a neutral, third-party verification of contract agreements submitted through the system.

1.5.24.2. Usage

When the DPC receives a fax or other electronic document from an individual, it creates an EDD Document record to store the document until it is picked up by the authorized recipients.

For fax documents, the recipients are specified by fax number and extension. For other electronic documents, the recipients are specified by electronic mail address. The DPC looks up an Organization record for each recipient by fax number and extension or e–mail address. If the record cannot be found, then the DPC looks in the Individual Biometric Database but only if the recipient is specified by e–mail address. For each recipient, the DPC creates a Recipient record that references both the Document and the recipient's biometric Identification specified by the Organization or IBD record if found. The DPC allows recipients who are not registered in the system, but it cannot then ensure delivery or confidentiality for those recipients.

The EDD is flexible enough to allow fax documents to be sent to an individual's e–mail address and e–mail messages sent to a fax machine.

While no electronic signature is placed on the document by the system, the system does guarantee through encryption that the message as received (and decrypted) by the Certified Email or Secure Fax terminal was sent by the individual.

Duly authorized officers of the organization can submit secure faxes or electronic messages to the DPC to assign title and fax extensions to new members, to update a member's title or fax extension, or to remove terminated members.

When an individual is removed from the organization tree, the DPC retires the extension number for a period of one year. This retirement period allows the individual sufficient time to inform confidants that he can no longer receive confidential faxes at that extension and so that the organization cannot mistakenly activate someone else at the extension who might then otherwise receive faxes not intended for him or her.

The EDD maintains an archive database which contains copies of Document and Recipient records when requested by the sender or one of the recipients of the document. The archive database is periodically moved onto CD–ROM.

1.5.24.3. Database Schema

The EDD has three record types:

Document Record:

documentNumber = int8
senderId = int4
documentFax = fax
documentText = text
messageKey = int8
status = int1

Recipient Record:

documentNumber = int8
recipientId = int4
recipientFaxNumber = char12
recipientFaxExtension = char8
recipientEmailAddr = text
receivedBy = int4
lastModified = time
deliveryStatus = int1
contractStatus = int1

Archive Request Record:

biometricId = int4
documentNumber = int8
requestorFaxNumber = char12
requestorFaxExtension = char8
requestorEmailAddr = text

Organization Record:

biometricId = int4
registeredBy = int4
company = text
title = text
faxNumber = char12
faxExtension = char8
emailAddr = text
activeDate = time
privs = int2
status = int1

The Document record status field is one of:

0: incomplete

1: ok

The Recipient record delivery status field is one of:

0: incomplete

1: notified

2: rejected

3: retrieved

4: retrieved unsecured

5: busy

The Recipient record contract status field is one of:

0: none

1: accepted

2: rejected

The Organization record status field is one of:

0: active

1: suspended

The Organization record privs** field is used to indicate what privileges the DPC allows that individual:

0: registration

The Document, Recipient, and Archive Retrieve records are keyed by documentNumber. The Organization records are keyed by biometricId. The EDD maintains secondary indexes on the Document senderId field, the Recipient recipientId field, and the Organization company name and title fields.

1.5.24.4. Database Size

The EDD's storage requirements depend primarily on the number of fax pages it will have to store since e-mail messages are relatively small compared to fax pages. Each fax page requires about 110 KB of storage.

Assuming 4 pages per fax, 2 faxes per person per day, and 30 million fax machines, the EDD requires 24 GB of storage to spool one day's worth of faxes.

1.5.24.5. Security

Documents are sent to and from the system encrypted using the BIA encryption mechanism. However, the encryption key is stored in the same database as the document. The document is left in its encrypted form to prevent casual disclosure, but individuals concerned about security of documents stored on the system should make some arrangement for additional encryption themselves.

1.5.24.6. Message Bandwidth

Each fax page requires about 110 KB which means that a T1 connection, with a throughput of 1.54 MBits/second, can handle about 1.75 fax pages per second.

1.5.25. Electronic Signature Database

1.5.25.1. Purpose

The Electronic Signature Database (ESD) authenticates and tracks all electronic signatures created by the system.

1.5.25.2. Usage

Individuals who are members of the system submit a 16–byte "message digest" for the document along with biometric–PICs and obtain a "digital signature" which remains on file with the system in perpetuity. This digital signature encodes the individual's name, biometric identification code, the authorized signature record number, document title, along with the timestamp at which the document was signed.

To verify a signature, a message digest for the document are first calculated (using RSA's MD5 for instance) and sent along with the document's signature tags. The ESD looks up the signature tags and validates the just recently calculated message digest against the message digest stored in the database.

1.5.25.3. Database Schema

The schema for the Electronic Signature record is:

Electronic Signature:
signatureNumber = int8
signer = int4
documentName = text
checksum = int16
date = time

The signer is the biometric identification code for the individual signing the document. The electronic signature record is hashed by signatureNumber.

1.5.25.4. Database Size

For each 1 GB of secondary storage, the Electronic Signature Database stores 27 million records (each record is about 32 bytes).

1.5.25.5. Dependencies

The ESD has dependencies on the signer's biometric Identification. Since these signatures remain valid essentially forever, ESD records are not removed when the system deletes the signer's Individual Biometric Database record. Note that this requires the IBD to never reuse a biometric Identification.

1.5.26. Remote Merchant Database

1.5.26.1. Purpose

The Remote Merchant Database (RMD) stores information on merchants that provide goods or services over telephones, cable television networks, or the Internet. Each order sent by an individual using a properly-equipped terminal is routed through the merchant's order terminal to the system.

1.5.26.2. Usage

Once an individual's remote transaction authorization is received and the MAC validated by the DPC, the merchant code is compared against the merchant code in the RMD. The merchant code, be it phone number, merchant-product credential, or internet address, exists in the RMD record under the correct merchant identification code or the DPC terminates the request and returns an invalid merchant code error to the sending BIA terminal device.

1.5.26.3. Database Schema

The schema for the Remote Merchant record is:

Remote Merchant:
- merchantId = int4
- merchantCode = char16
- merchantType = int1
- publicKey = int16

The Remote Merchant merchantType is one of:
- 0: telephone
- 1: CATV
- 2: Internet

The merchantId and merchantCode are both primary keys. No two RMD records have the same merchantId and merchantCode combination.

1.5.26.4. Database Size

Assuming about 100,000 remote merchants, the RMD requires about 24 bytes per record for a total of about 2.4 MB storage required.

1.5.26.5. Dependencies

The RMD does not have any direct dependencies on any other DPC components.

1.5.27. System Performance

The key performance number is how many financial authorization transactions the DPC handles per second.

In GM:

1. MACM checks the MAC (local)
2. SNM checks the sequence number (network message)
3. MDM decrypts the biometric–PIC block (local)
4. Find IBD machine (local)
5. Send identify request to the IBD machine (network message)

In IBD machine:

6. Retrieve all IBD records for the PIC (x seeks and x reads, where x is the number of pages required to store the biometric records).
7. For each record, compare against its primary biometric (y / 2 ms where y is the number of records retrieved).
8. If no reasonable match, repeat step 9 but compare against the secondary biometric (z * y / 2 ms, where y is the number of records retrieved and z is the probability no match is found).
9. Update the best matching IBD record's checksum queue and check for possible replay attacks (1 seek, 1 read, and 1 write).

10. Return the best matching IBD record or an error if the match is not close enough (network message).

In GM:

11. Authorize request with an external processor (network message)
12. GM encrypts and MACs the response (local).
13. Sends response packet back (network message).

Total Disk Costs:

$x * (s + r) + y / 2 * (1 + z) + s + r + w + 5 * n$

$= (x + 1) * (s + r) + y / 2 * (1 + z) + w + 5 * n$

[assume x is 20, y is 30, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 21 * 10 ms + 15 * 1.05 ms

= 226 ms

= 4.4 TPS

[assume x is 10, y is 15, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 11 * 10 ms + 7.5 * 1.05 ms

= 118 ms

= 8.4 TPS

[assume x is 1, y is 1, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 2 * 10 ms + 1/2 * 1.05 ms

= 21 ms

= 47 TPS

The backup IBD machine also processes requests doubling effective TPS.

Worst case (with 2 machines in use):

Individuals per PIC	TPS
30	8
15	16
1	94

Average case (with 20 machines in use):

Individuals per PIC	TPS
30	88
15	168
1	940

Best case (with 40 machines in use):

Individuals per PIC	TPS
30	176
15	336
1	1880

The above is just an example of one configuration of the system as it could be implemented in a commercially viable manner. However, it is anticipated that this invention can be configured in many other ways which could incorporate the use of faster computers, more computers and other such changes.

1.6. Terminal Protocol Flowchart

The following set of protocol flows describe interactions between specific terminals, the DPC, the attached BIA, and other parties such as the credit/debit processor, and so on.

1.6.1. Retail Point of Sale Terminal

In this case, an RPT communicates with a retail BIA and the DPC to authorize a transaction. The transaction amount is 452.33, the individual's account is 4024–2256–5521–1212 merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

RPT → BIA Set Language <English>
BIA → RPT Ok
RPT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner

BIA → RPT Ok
RPT → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → RPT Ok
RPT → BIA Get Account Number <40>
BIA/LCD: <Now enter your account index code, then press <enter>>
Individual enters code, then <enter>
BIA → RPT Ok
RPT → BIA Validate Amount <452.33> <40>
BIA/LCD: <Amount 452.33 OK?>
Individual enters OK
BIA → RPT Ok
RPT → BIA Assign Register <1> <123456>
BIA → RPT Ok
RPT → Form Message <transaction>
BIA → RPT <Transaction Request Message>
BIA → RPT OK
BIA/LCD: <I'm talking to DPC Central>
RPT → DPC <Transaction Request Message>
DPC: validate biometric, retrieve account number → 4024–2256– 5521–1212
DPC → VISA <authorize 4024–2256–5521–1212 452.33 123456>
VISA → DPC <ok 4024–2256–5521–1212 452.33 123456 autho–code>
DPC: get private code
DPC → RPT <Transaction Response Message>
RPT → BIA Show Response <Transaction Response Message> <8>
BIA/LCD: <Transaction ok: I am fully persuaded of it>
BIA → RPT <Ok <autho–code>>
RPT: prints receipt with autho–code on it

1.6.2. Internet Point of Sale Terminal

In this case, an IPT communicates with a standard BIA and the DPC to authorize a transaction. The transaction amount is 452.33, the individual's account is 4024–2256–5521–1212, the internet merchant is located

at merchant.com, his merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

IPT → merchant.com <send me merchant code if resources available>
merchant.com → IPT <ok 123456 merchant.com–public–key>
IPT generates session key, encrypted with merchant.com–public– key
IPT → merchant.com <session key>
All subsequent communications with merchant are encrypted with session key.
merchant.com → IPT <price and product information>
IPT/Screen: displays price and product information
Individual: selects item "fruitcake, price 45.33"
IPT → BIA Set Language <English>
BIA → IPT Ok
IPT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → IPT Ok
IPT → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → IPT Ok
IPT → BIA Get Account Number <40>
BIA/LCD: <Now enter your account index code, then press <enter>>
Individual enters code, then <enter>
BIA → IPT Ok
IPT → BIA Validate Amount <45.33> <40>
BIA/LCD: <Amount 45.33 OK?>
Individual enters OK
BIA → IPT Ok
IPT → BIA Assign Register <1> <123456>
BIA → IPT Ok
IPT → BIA Assign Register <2> <merchant.com>
BIA → IPT Ok
IPT → BIA Assign Register <3> <fruitcake>
BIA → IPT Ok
IPT → BIA Form Message <remote transaction>

BIA → IPT <Remote Transaction Request Message>
BIA → IPT OK
BIA/LCD: <I'm talking to DPC Central>
IPT → merchant.com <Remote Transaction Request Message>
merchant.com → secure–connect to DPC using DPC public key
merchant.com → DPC <Remote Transaction Request Message>
DPC: validate biometric, retrieve account number → 4024–2256– 5521–1212
DPC: validate internet merchant.com with code 123456
DPC → VISA <authorize 4024–2256–5521–1212 45.33 123456>
VISA → DPC <ok 4024–2256–5521–1212 45.33 123456 autho– code>
DPC: get private code
DPC → merchant.com <Transaction Response Message>
merchant.com stores autho code
merchant.com → IPT <Transaction Response Message>
IPT → BIA Show Response <Transaction Response Message> <8>
BIA/LCD: <Transaction ok: I am fully persuaded of it>
BIA → IPT <Transaction ok>

1.6.3. Internet Teller Terminal

In this case, an ITT communicates with a standard BIA, the DPC, and a bank's internet server to perform routine and nonroutine home banking operations. Note that the DPC isn't involved in actually validating any transactions, but is only responsible for creating a valid set of network credentials and securing the communications line to the bank.

ITT → bank.com <send me bank code if resources available>
bank.com → ITT <ok 1200>
ITT → BIA Set Language <English>
BIA → ITT Ok
ITT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → ITT Ok
ITT → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>
BIA → ITT Ok
RPT → BIA Get Account Number <40>
BIA/LCD: <Now enter your account index code, then press <enter>>
Individual enters code, then <enter>
BIA → ITT Ok
ITT → BIA Assign Register <1> <1200> (bank code)
BIA → ITT Ok
ITT → BIA Assign Register <2> <bank.com>
BIA → ITT Ok
ITT → BIA Assign Register <3> <ITT.port, bank.com.port> (TCP/IP addresses)
BIA → ITT Ok
ITT → Form Message <net credential>
BIA → ITT <network credential Request>
BIA → ITT Ok
BIA/LCD: <I'm talking to DPC Central>
ITT → DPC <network credential Request>
DPC: validate biometric, create credential(time, acct, bank)
DPC: get private code
DPC → ITT <network credential Response>
ITT → BIA Show Response <network credential Response>
BIA decrypt response, check response
BIA/LCD: <Credential ok: I am fully persuaded of it>
BIA encrypt credential, session key, challenge key with bank's public key
BIA → ITT <Secure Connection Request Message>
BIA → ITT <Session Key>
BIA → ITT Ok
BIA/LCD: <Secure connection to bank.com in progress>
ITT → bank.com <Secure Connection Request Message>
bank.com decrypt with private key, validate credential, use shared key
bank.com → ITT <ok>

Further transactions over the ITT → bank.com connections are all encrypted by the ITT using the ITT/bank session key.

Any transactions that the bank determines are non–routine must be validated by the individual using the BIA's challenge–response mechanism.

The challenge–response mechanism is available only while the BIA remains in the "secure connection" state.

bank.com → ITT <validate <validation request>>
ITT → BIA Validate Private <encrypted validation request>
BIA decrypts challenge section, and displays it
BIA/LCD: <Please OK: transfer of 12,420.00 to 1023–3302– 2101–1100>
Individual enters Ok
BIA re–encrypts response using challenge key
BIA/LCD: <Secure connection to bank.com in progress>
BIA → ITT <Ok <encrypted validation response>>
ITT → bank.com <encrypted validation response>

1.6.4. Electronic Signature Terminal

In this case, an EST communicates with a standard BIA and the DPC to construct digital signatures. The individual's private code is "I am fully persuaded of it" and the document to be signed is called "The Letter of Marque."

CET → BIA Set Language <English>
BIA → CET Ok
CET → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → CET Ok
CET → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → CET Ok
CET → BIA Validate Document <Letter of Marque> <40>
BIA/LCD: <Document "Letter of Marque" OK?>
Individual enters OK
BIA → CET Ok
CET → BIA Assign Register <1> <document MD5 value>
BIA → CET Ok

CET → Form Message <signature submit>
BIA → CET <Electronic Signature Request>
BIA → CET OK
BIA/LCD: <I'm talking to DPC Central>
CET → DPC <Electronic Signature Request>
DPC: validate biometric, create signature, return sig text code
DPC: get private code
DPC → CET <Electronic Signature Response>
CET → BIA Show Response <Electronic Signature Response> <8>
BIA/LCD: <Document ok: I am fully persuaded of it>
BIA → CET <Ok <sig text code>>

1.6.5. Certified Email Terminal

In this case, a CET communicates with a standard BIA and the DPC to transmit certified electronic mail. The individual's private code is "I am fully persuaded of it", and the document name is "Post Captain."

CET → BIA Set Language <English>
BIA → CET Ok
CET → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → CET Ok
CET → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → CET Ok
CET → BIA Validate Document <Post Captain> <40>
BIA/LCD: <Document "Post Captain" OK?>
Individual enters OK
CET/Screen: <Recipient list? >
Individual enters <fred@telerate.com joe@reuters.com>
CET → BIA Assign Register <1> <fred@telerate.com joe@reuters.com>
BIA → CET Ok
CET → Form Message <document submit>

BIA → CET <Electronic Document Submit Request>
BIA → CET OK
BIA/LCD: <I'm talking to DPC Central>
CET → DPC <Electronic Document Submit Request>
DPC: validate biometric, create message, return message #001234
DPC: get private code
DPC → CET <Electronic Document Submit Response>
CET → BIA Show Response <Electronic Document Submit Response> <8>
BIA/LCD: <Document ok: I am fully persuaded of it>
BIA → CET <Document ok <1234>>
CET → DPC <Electronic Document Data Request, 1234, section 1, incomplete>
DPC → CET <Electronic Document Data Response, incomplete>
CET → DPC <Electronic Document Data Request, 1234, section 2, incomplete>
DPC → CET <Electronic Document Data Response, incomplete>
CET → DPC <Electronic Document Data Request, 1234, section 3, incomplete>
DPC → CET <Electronic Document Data Response, incomplete>
CET → DPC <Electronic Document Data Request, 1234, section 4, done>
DPC → CET <Electronic Document Data Response, track 1234.1 1234.2>
DPC → fred@telerate.com <email 1234.1 message arrived>
DPC → joe@reuters.com <email 1234.2 message arrived>
mailer@telerate.com → DPC <received notification email for 1234.1>
DPC → sender@company.com <email 1234.1 recipient notified>
mailer@reuters.com → DPC <received notification email for 1234.2>
DPC → sender@company.com <email 1234.2 recipient notified>

[At Fred's CET: Fred sees the "message arrived" electronic mail message, and decides to go pick up the message]

CET → BIA Set Language <English>
BIA → CET Ok
CET → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → CET Ok
CET → BIA Get Pin <40> BIA/LCD: <Please enter your PIC>
Individual enters PIC, then <enter>

BIA → CET Ok
CET → BIA Assign Register <1> <1234.1>
BIA → CET Ok
CET → Form Message <document retrieve>
BIA → CET <Electronic Document Retrieve Request>
BIA → CET OK
BIA/LCD: <I'm talking to DPC Central>
CET → DPC <Electronic Document Retrieve Request>
DPC: validate biometric, lookup 1234.1
DPC: get private code
DPC → CET <Electronic Document Retrieve Response>
CET → BIA Show Response <Electronic Document Retrieve Response> <8>
BIA/LCD: <Document ok: I am fully persuaded of it>
BIA → CET <Document ok <message key>>
CET/Screen: decrypt, then show document

1.6.6. Secure Fax Terminal

In this case, a SFT communicates with an BIA/catv and the DPC to transmit secure faxes.

SFT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → SFT Ok
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
SFT → BIA Set Pin <40>
BIA/LCD: <Please enter your Title Index, then press <enter>>
Individual enters title index, then <enter>
SFT → BIA Set Title Index Code <40>
BIA → SFT Ok
SFT/Screen: <Recipient? (add * for ext, # at end)>
Individual enters <1 510 944–6300*525#)
SFT/Screen: <Recipient? (add * for ext, # at end)>
Individual enters <1 415–877–7770#>

SFT/Screen: <Recipient? (add * for ext, # at end)>
Individual enters <#>
SFT → BIA Assign Register <1> <15109446300*525 14158777770>
BIA → SFT Ok
SFT → Form Message <document submit>
BIA → SFT <Secure Fax Submit Request>
BIA → SFT OK
BIA/LCD: <I'm talking to DPC Central>
SFT → DPC <Secure Fax Submit Request>
DPC: validate biometric, create message, return message #001234
DPC: get private code
DPC → SFT <Secure Fax Submit Response>
SFT → BIA Show Response <Secure Fax Submit Response> <10>
BIA/LCD: <Document ok: I am fully persuaded of it>
BIA → SFT <Document ok <001234>>
SFT → DPC <Secure Fax Data Request, 1234, section 1, incomplete>
DPC → SFT <Secure Fax Data Response, incomplete>
SFT → DPC <Secure Fax Data Request, 1234, section 2, incomplete>
DPC → SFT <Secure Fax Data Response, incomplete>
SFT → DPC <Secure Fax Data Request, 1234, section 3, incomplete>
DPC → SFT <Secure Fax Data Response, incomplete>
SFT → DPC <Secure Fax Data Request, 1234, section 4, done>
DPC → SFT <Secure Fax Data Response>
DPC → connect–fax 15109446300
DPC → SFT6300 <fax–cover "Sam Spade" from "Fred Jones" 1234.1 4 pages waiting>
DPC → disconnect
DPC → connect–fax 14158777770
DPC → SFT7770 <fax–cover "John Jett" from "Fred Jones" 1234.2 4 pages waiting>
DPC → disconnect

[At Sam's SFT: Sam sees document fax cover arrive from Fred, initiates retrieval of document from DPC using tracking code 1234.1.]

SFT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual (Sam) places finger on scanner

BIA → SFT Ok
SFT → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual (Sam) enters PIC, then <enter>
BIA → SFT Ok
SFT → BIA Assign Register <1> <1234.1>
BIA → SFT Ok
SFT → Form Message <document retrieve>
BIA → SFT <Secure Fax Retrieve Request>
BIA → SFT OK
BIA/LCD: <I'm talking to DPC Central>
SFT → DPC <Secure Fax Retrieve Request>
DPC: validate biometric, lookup 1234.1, verify biometric=PIC = Sam Spade
DPC: lookup private code in database
DPC → SFT <Secure Fax Retrieve Response>
SFT → BIA Show Response <Secure Fax Retrieve Response> <8>
BIA → SFT <Document ok: I am fully persuaded of it <message key>>
SFT/Screen: <Document ok: I am fully persuaded of it>
SFT/Screen: print fax

1.6.7. Biometric Registration Terminal

In this case, a BRT communicates with a registration BIA and the DPC to register an individual with the system.

BRT → BIA Set Language <English>
BIA → BRT Ok
BRT → BIA Get Biometric <20> <primary>
BIA/LCD: <Please place PRIMARY finger on lighted panel>
Individual places primary finger on scanner
BIA → BRT Ok
BRT → BIA Get Biometric <20> <secondary>
BIA/LCD: <Please place SECONDARY finger on lighted panel>
Individual places secondary finger on scanner
BIA → BRT Ok
BRT → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters 123456, then <enter>

BIA → BRT Ok

BRT → BIA Get Message Key

BIA → BRT <Ok <message key>>

BIA → <Registration Request Message>

BRT/Screen: <Name: >

Representative enters <Fred G. Shultz>

BRT/Screen: <Address: >

Representative enters <1234 North Main>

BRT/Screen: <Zipcode: >

Representative enters <94042>

BRT/Screen: <Private code: >

Representative queries individual, then enters <I am fully persuaded of it.>

BRT/Screen: <Asset account list: >

Representative enters <2, 1001–2001–1020–2011> (credit card)

Representative enters <3, 1001–1002–0039–2212> (checking account)

BRT/Screen: <Emergency account: >

Representative enters <1, 1001–1002–0039–2212> (emergency, checking account)

BRT → Form Message <registration>

BIA → BRT <Registration Request Message>

BIA → BRT OK

BIA/LCD: <I'm talking to DPC Central>

BRT appends message–key–encrypted personal information to request

BRT → DPC Registration Request Message> <encrypted personal information>

DPC: verify PIC 123456

DPC → BRT <Registration Response Message>

BRT → BIA Show Response <Registration Response Message> <8>

BIA/LCD: <Registration ok: I am fully persuaded of it, 123456>

BIA → BRT <Ok>

1.6.8. Customer Service Terminal

In this case, a CST communicates with a standard BIA and the DPC to verify the identity and the credentials of an individual.

CST → BIA Set Language <English>
BIA → CST Ok
CST → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → CST Ok
CST → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → CST Ok
CST → BIA Get Message Key
BIA → CST <Ok <message key>>

CST → Form Message <Individual Identity Request>
BIA → CST <Individual Identity Request>
BIA → CST OK
BIA/LCD: <I'm talking to DPC Central>
CST → DPC <Individual Identity Request>
DPC: get private code, individual's priv
DPC → CST <Individual Identity Reply>
CST → BIA Show Response <Individual Identity Reply> <8>
BIA/LCD: <Identity ok: I am fully persuaded of it>
BIA → CST <Ok <individual-name priv>>
CST: check priv to see if sufficient for CST use

1.6.9. Issuer Terminal

In this case, an IT communicates with a standard BIA and the DPC to authorize and send a batch of account addition and deletion requests to the DPC. The individual's private code is "I am fully persuaded of it", and the bank code is 1200.

IT → BIA Set Language <English>
BIA → IT Ok
IT → BIA Get Biometric <20>
BIA/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → IT Ok
IT → BIA Get Pin <40>
BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters PIC, then <enter>
BIA → IT Ok
IT → BIA Assign Register <1> <1200>
BIA → IT Ok
IT → BIA Get Message Key
BIA → IT <message key>
BIA → IT Ok
IT → BIA Form Message <issuer request>
BIA → IT <Issuer Batch Request>
BIA → IT OK
BIA/LCD: <I'm talking to DPC Central>
IT → DPC <Issuer Batch Request> <message–key–encrypted issuer batch>
DPC: validate biometric, validate bank code 1200 vs. BIA identification
DPC: get private code
DPC: decrypt message using message key, execute issuer batch
DPC → IT <Issuer Batch Reply>
IT → BIA Show Response <Issuer Batch Reply> <8>
BIA/LCD: <Batch ok: I am fully persuaded of it>
BIA → IT <Ok>

1.6.10. Automated Teller Machinery

In this case, an ATM communicates with an integrated ATM BIA and the DPC to identify an individual and obtain his bank account number. The individual's account is 2100–0245–3778–1201, bank code is 2100, and the individual's private code is "I am fully persuaded of it."

ATM → BIA Get Biometric <20>
ATM/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → ATM Ok
ATM/LCD: <Please enter your PIC, then press <enter>>
Individual enters 123456 on ATM keyboard, then <enter>
ATM → BIA Set Pin <123456>
BIA → ATM Ok
ATM/LCD: <Now enter your account index code, then press <enter>>
Individual enters 2, then <enter>
ATM → BIA Set Account Index Code <2>
BIA → ATM Ok
ATM → BIA Assign Register <1> <2100>
BIA → ATM Ok
ATM → Form Message <account access>
BIA → ATM <Account Access Request Message>
BIA → ATM OK
ATM/LED: <I'm talking to DPC Central>
ATM → DPC <Account Access Request Message>
DPC: validate biometric, retrieve account number →2100– 0245–3778–1201
DPC: get private code
DPC → ATM <Account Access Response Message>
ATM → BIA Decrypt Response <Account Access Response Message>
BIA → ATM <2100–0245–3778–1201> <no emergency> <I am fully persuaded of it>
ATM/LCD: <I am fully persuaded of it>

At this point, the ATM has the account number it needs to continue, so it then retrieves the information associated with the account number, and commences interacting with the individual.

1.6.11. Phone Point of sale Terminal

In this case, a PPT communicates with an integrated phone BIA and the telephone merchant to download information and purchase items securely using the telephone. The individual's PIC is 1234, the account index

code is 1, the merchant's phone number is 1 800 542–2231, merchant code 123456, and the actual account number is 4024–2256–5521– 1212.

Note that the telephone strips the area code (1–800) from the telephone number before handing it to the system.

Individual dials phone 18005422231
PPT → connect merchant 18005422231
PPT → BIA Assign Register 1 <5422231>
Sales rep answers. Individual selects item "fruitcake". Sales rep downloads info.
merchant → PPT <123456 fruitcake 43.54>
PPT → BIA Get Biometric <20>
Phone/LCD: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → PPT Ok
Phone/LCD: <Please enter your PIC, then press #>
Individual enters 1234 on keypad, then # or * (enter)
PPT → BIA Set Pin <1234>
BIA → PPT Ok
Phone/LCD: <Now enter your account index code>
Individual enters 1, then <enter>
RPT → BIA Set Account index code <1>
BIA → PPT Ok
RPT → BIA Assign Register <2> <123456>
BIA → PPT Ok
Phone/LCD: <Press # if amount 45.54 is ok>
Individual enters # (yes)
PPT → BIA Set Amount <43.54>
BIA → PPT Ok
PPT → Form Message <remote transaction>
BIA → PPT <Remote Transaction Request>
BIA → PPT Ok
Phone/LCD: <I'm talking to DPC Central>
PPT → merchant <Phone Transaction Request>
merchant → DPC secure–connect to DPC using DPC–public–key
merchant → DPC <Phone Transaction Request>

DPC: validate biometric, retrieve account number → 4024– 2256–5521–1212
DPC: validate merchant 5422231 has code 123456
DPC → VISA <authorize 4024–2256–5521–1212 43.54 123456>
VISA → DPC <ok 4024–2256–5521–1212 43.54 123456 autho– code>
DPC: get private code
DPC → merchant <Transaction Response Message>
merchant examines response code
merchant → PPT <Transaction Response Message>
PPT → BIA Decrypt Message <Transaction Response Message>
BIA → PPT <Ok <I am fully persuaded of it> <autho–code>>
Phone/LCD: <chime> Transaction ok: I am fully persuaded of it

1.6.12. Cable–TV Point of sale Terminal

In this case, a CPT communicates with an integrated cable–tv BIA and the Cable television merchant to download information and purchase items securely using the cable television broadband network. The individual's PIC is 1234, the account index code is 1, the channel is 5, the merchant code 123456, and the actual account number is 4024–2256–5521– 1212.

Individual turns the television to channel 5.
merchant → CPT <fruitcake 43.54 123456> (broadcast)
Individual hits "buy" on TV Remote
CPT/TV: <Buying fruitcake for $43.54>
CPT → BIA Get Biometric <20>
CPT/TV: <Please place finger on lighted panel>
Individual places finger on scanner
BIA → CPT Ok
CPT/TV: <Please enter your PIC, then press <enter>>
Individual enters 1234 on keypad, then "buy"
CPT → BIA Set Pin <1234>
BIA → CPT Ok
CPT/TV: <Now enter your account index code>
Individual enters 1, then <enter>
RPT → BIA Set Account index code <1>
BIA → CPT Ok

RPT → BIA Assign Register <1> <channel 5, 15:30:20 PST>
BIA → RPT Ok
CPT → BIA Assign Register <2> <123456>
BIA → CPT Ok
CPT/TV: <Press "buy" if amount 45.54 is ok>
Individual enters "buy"
CPT → BIA Set Amount <43.54>
BIA → CPT Ok
CPT → Form Message <CableTV transaction>
BIA → CPT <CableTV Transaction Request>
BIA → CPT Ok
CPT/TV: <I'm talking to DPC Central>
CPT → CTV Center <CableTV Transaction Request>
CTV Center → merchant <CableTV Transaction Request>
merchant → DPC secure-connect to DPC using DPC-public-key
merchant → DPC <CableTV Transaction Request>
DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
DPC: validate merchant channel 5, current show has code 123456
DPC → VISA <authorize 4024-2256-5521-1212 43.54 123456>
VISA → DPC <ok 4024-2256-5521-1212 43.54 123456 antho- code>
DPC: get private code, mailing address
DPC → merchant <Transaction Response Message>
merchant examines response code, records mailing address
merchant → CTV Center <Transaction Response Message>
CTV Center → CPT <Transaction Response Message>
CPT → BIA Decrypt Message <Transaction Response Message>
BIA → CPT <Ok <I am fully persuaded of it> <antho-code>>
CPT/TV: <chime> Transaction ok: I am fully persuaded of it

From the foregoing, it will be appreciated how the objects and features of the invention are met.

First, the invention provides a computer identification system that eliminates the need for a user to possess and present a physical object, such as a token, in order to initiate a system access request.

Second, the invention provides a computer identification system that is capable of verifying a user's identity, as opposed to verifying possession of proprietary objects and information.

Third, the invention verifies the user's identity based upon one or more unique characteristics physically personal to the user.

Fourth, the invention provides an identification system that is practical, convenient, and easy use.

Fifth, the invention provides a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

Sixth, the invention provides a computer identification system that enables a user to notify authorities that a particular access request is being coerced by a third party without giving notice to the third party of the notification.

Seventh, the invention provides an identification system that allows for identification of the sender and recipient of an electronic message and/or facsimile.

Although the invention has been described with respect to a particular tokenless identification system and method for its use, it will be appreciated that various modifications of the apparatus and method are possible without departing from the invention, which is defined by the claims set forth below.

5. GLOSSARY

ACCOUNT INDEX CODE:

A digit or an alpha–numeric sequence that corresponds to a particular financial asset account

AID:

Authorized Individual Database: contains the list of individuals authorized to use personal and issuer BIA devices.

AOD:

Apparatus Owner Database: central repository containing the geographic and contact information on the owner of each BIA.

ASCII:

American Standard Code for Information Interchange

ATM:

Automated Teller Machinery; uses encoded biometric identity information to obtain access to a financial asset management system, including cash dispensing and account management.

BIA:

Biometric input apparatus; collects biometric identity information, encodes and encrypts it, and makes it available for authorizations. Comes in different hardware models and software versions.

Biometric:

A measurement taken by the system of some aspect of an individual's physical person.

Biometric ID:

An identifier used by the system to uniquely identify an individual's biometric record (IRID – Individual Record ID)

BIO–PIC GROUP:

A collection of algorithmically dissimilar biometric samples linked to the same personal identification code

BRT:

Biometric Registration Terminal; located at retail banking outlets, BRTs combine biometric registration information with an individual–selected PIN and selected personal information to register individuals with the system.

CBC:

Cipher Block Chaining: an encryption mode for the DES.

CCD:

Charged–Coupled Device

CET:

Certified Email Terminal; uses BIA to identify sender, encrypts document, sends to system. System retains, notifies recipient of message arrival in–system. Recipient identifies self, and then document is transmitted to recipient. Notification to transmitter once document is sent. Document is verified sent, secured by BIA encryption. Transmitter may inquire as to delivery status. Both participants must be system members.

COMMANDS:

A program or subroutine residing in the DPC that performs a specific task, activated by a request message sent from a BIA-equipped terminal.

CONTRACT ACCEPT/REJECT:

The process by which an individual enters their BIO–PIC and instructs the DPC to register said individual's contractual acceptance or rejection of the terms contained within a document which had been sent by electronic facsimile to that individual.

CPT:

Cable–TV Point–of–Sale Terminal: combines an onscreen display simulcast digital signal informing TV–top cable box of product information with product video, and an BIA controller remote which performs the biometric–pin validation using the CATV communications network. Order/autho/mailing–address/item–id forwarded to merchant. Results of authorization are displayed on the TV.

CST:

Customer Service Terminals; provide system customer service personnel with varying degrees of access (based on access privilege) the ability to retrieve and modify information on individuals in order to help people with account problems.

DATA SEALING STEP:

The conversion of plain text to cipher text (known as "encryption") in combination with the encrypted checksumming of a message that allows information to remain in plain text while at the same time providing a means for detecting any subsequent modification of the message.

DES:

Digital Encryption Standard: a standard for the cryptographic protection of digital data. See standard ANSI X3.92–1981

DETERMINATION:

The status of the command processed during the execution step.

DPC:

A data processing center, namely, the place and the entity where the hardware, software, and personnel are located with the goal of supporting a multigigabyte biometric identity database. A DPC processes electronic messages, most of which involve performing biometric identity checks as a precursor to performing some action, such as a financial transfer, or sending a fax, or sending electronic mail, etc.

DSP:

Digital Signal Processor: a class of integrated circuits that specialize in the mathematical operations required by the signal processing applications.

DUKPT:

Derived Unique Key Per Transaction: See standard ANSI/ABA X9.24–1992

EDD:

Electronic Document Database: central repository containing all pending faxes and electronic messages awaiting pickup by individuals.

EMERGENCY ACCOUNT INDEX:

The alpha–numeric digit or sequence selected by an individual which, when accessed, will result in a transaction being labeled by the system as an emergency transaction, potentially causing the display of false screens and/or the notification of authorities that said individual has been coerced into performing a transmission or transaction.

ESD:

Electronic Signature Database: central repository containing all MD5 and electronic signatures of all documents signed by anybody, referenced by authorization number.

EST:

Electronic Signature Terminal; uses BIA to identify individual, computer calculates checksum on document, sends checksum to system, system validates, timestamps, saves checksum, and returns with sig code. Uses Internet as transport. EST also verifies signatures given a sig code and an MD5 calculation.

FAR (False Accept Rate):

The statistical likelihood that one individual's biometric will be incorrectly identified as the biometric of another individual.

FALSE SCREENS:

Displays of information which has been intentionally pre– determined to be subtly inaccurate such that a coercing party will not illegally obtain accurate data about an individual's financial assets, all the while remaining unaware of the alteration of the information.

FDDI:

Fiber Digital Device Interface: a networking device that utilizes a fiber optic token ring.

FS:

Field Separator

FW:

Firewall Machine: the internet–local net router that regulates traffic into and out of the DPC.

GM:

Gateway Machine: the main processing computers in the DPC; runs most of the software.

IBD:

Individual Biometric Database: central repository for biometric, financial asset, and other personal information. Queries against the biometric database are used to verify identity for transaction authorizations and transmissions.

ID:

Issuer Database: central repository containing the institutions that are allowed to add and delete financial asset account numbers with the system.

IML:

IBD Machine List: a software module in the DPC determines which IBD machines are responsible for which PIN codes.

INTERNET MERCHANT:

A retail account selling services or good to consumers by means of the Internet electronic network

IPT:

Internet Point–of–Sale Terminal: items and merchant code from the internet, BIA biometric–PIN for validation, sent to system using Internet, autho/order/PO # forwarded to merchant. System response using internet as well, displaying results on screen.

ISSUER:

A financial account issuer for financial assets to be registered with the DPC.

ISSUER BATCH:

A collection of "add" and "delete" instructions complete with biometric IDs, financial asset accounts, and account index codes verified and submitted by an issuer to the DPC.

IT:

Issuer Terminals; provides a batch connection to the system for issuers to add and remove (their own) financial asset account numbers from specific individual's IBD records.

ITT:

Internet Teller Terminal; authorizes network terminal session using encrypted credential obtained from DPC using biometric ID.

LCD:

Liquid Crystal Display: a technology used for displaying text.

MAC:

Message Authentication Code: an encrypted checksum algorithm, the MAC provides assurance that the contents of a message have not been altered subsequent to the MAC calculation. See standard ANSI X9.9–1986

MACM:

Message Authentication Code Module: a software module in the DPC that handles MAC validation and generation for inbound and outbound packets.

MDM:

Message Decrypt Module: a software module in the DPC that encrypts and decrypts packets from or destined to an BIA device.

MPM:

Message Processing Module: a software module in the DPC that performs the processing of request packets.

NETWORK CREDENTIAL:

Both the individual and the bank are identified by the DPC to create the network credential. The credential includes the individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports). DPC creates a network credential using the individual's account id, the time of day, and the bank code. The DPC signs this credential using Public Key Encryption and the DPC's Private Key.

PFD:

Prior Fraud Database: central repository for IBD records which have had prior fraud associated with them. Every new customer's biometrics are checked against all PFD records with the intent of reducing recidivism.

PGL:

PIN Group List: a software module in the DPC that is responsible for maintaining the configuration of the IBD machines.

PIN:

Personal Identification Number; a method for protecting access to an individual's account through secret knowledge, formed from at least one number.

PIC:

Personal Identification Code; a PIN formed from either numbers, symbols, or alphabetic characters.

POS:

Point–Of–Sale; a place where goods are sold.

PPT:

Phone Point–of–Sale Terminal; combines phone number with merchant price and product information to authorize a transaction over a BIA-equipped telephone. Order/authorization/mailing–address/PO forwarded to merchant. Resulting authorization is displayed on phone LCD, or "spoken", along with the individual's private code.

RAM:

Random Access Memory

RF:

Radio Frequency: generally refers to radio frequency energy emitted during the normal operation of electrical devices.

REGISTERS:

Memory reserved for a specific purpose, data set aside on chips and stored operands to instructions

REQUESTS:

Electronic instructions from the BIA to DPC instructing the DPC to identify the individual and thereby process the individual's command in the event the identification is successful

RMD:

Remote Merchant Database: contains all merchant identification codes for merchant telephone and Cable TV order shops; indexed by merchant ID. Contains per–merchant system encryption codes as well.

RPT:

Retail Point–of–Sale Terminal; combines encoded biometric identity information with retail transaction information (possibly from an electronic cash register) and formulates authorization requests of the system using X.25 networks, modems, etc.

SECURE TRANSMISSION:

An electronic message or facsimile wherein at least one party has been identified by the DPC.

SFT:

Secured Fax Terminal; uses BIA to identify sender, sends fax either unsecured, sender–secured, secured, or secured–confidential. The latter two require recipients to identify themselves using biometric–PIN. Uses "titles" (specified using a title index digit) to label outbound faxes. Sender may inquire as to delivery status. Both participants must be system members. Either sender or recipient can request that the fax be archived.

SNM:

Sequence Number Module: a software module in the DPC that handles the DUKPT sequence number processing for inbound request packets. Sequence number processing protects against replay attacks.

Terminal:

A device that uses the BIA to collect biometric samples and form request messages that are subsequently sent to the DPC for authorization and execution. Terminals almost always append ancillary information to request messages, identifying counterparties and the like.

TITLE INDEX CODE:

Alpha–numeric sequence uniquely identifying an individual's authorized role or capacity within the context of his employment

Token:

An inanimate object conferring a capability.

TRACKING CODE:

An alpha–numeric sequence assigned to data stored in or transmitted by the DPC, such that said sequence may be used to recall the data or obtain a report on the status of the transmission of the data.

TRANSACTION:

An electronic financial exchange

TRANSMISSION:

An electronic message other than an electronic financial exchange

VAD:

Valid Apparatus Database: central repository in which each BIA (with associated unique encryption codes) is identified, along with the owner of the BIA.

I claim:

1. A voluntary tokenless identification computer system for determining an individual's identity from an examination of at least one biometric sample and a personal identification code gathered during a bid step, and comparison with previously recorded biometric sample and personal identification code gathered during a registration step, said system comprising:
    a. at least one computer;
    b. first gathering and display means for voluntary input of at least one biometric sample, personal identification code, and private code from an individual during the registration step, wherein the private code is selected by the individual;
    c. second gathering and display means for voluntary input of at least one biometric sample and personal identification code, from an individual during a bid step;
    d. first interconnecting means for interconnecting said first and second gathering and display means to said computer for transmitting the gathered biometric sample, personal identification code, and private code from said first and second gathering means to said computer;
    e. means for comparison of biometric sample and personal identification code gathered during the bid step with the biometric sample and personal identification code gathered during the registration step, for producing an evaluation;
    f. execution means within said computer for storage of data and processing and execution of commands for producing a determination; and
    g. means for output of said evaluation, determination, or private code from said computer.
2. The apparatus of claim 1 wherein the computer comprises means for detecting and preventing electronic intrusion of the computer system.
3. The apparatus of claim 1 wherein the computer is placed remote from the gathering and display means.
4. The apparatus of claim 1, the first and second gathering and display means further comprising;
    a. at least one biometric input means for gathering biometric samples further comprising a hardware and software component;
    b. at least one terminal means that is functionally partially or fully integrated with the biometric input means for input of and appending additional data;

c. at least one data entry means for input of a personal identification code where in said means is integrated either with the biometric input means or the terminal means; and

d. second interconnecting means for interconnecting said biometric input means, data entry means and said terminal.

5. The apparatus of claim 4 wherein said terminal further comprises at least one display means for display of data.

6. The apparatus of claim 4 wherein the biometric input means has a hardware identification code previously registered with the computer, which makes the biometric input means uniquely identifiable to the computer.

7. The apparatus of claim 4 wherein the hardware component further comprises:

a. at least one computing module for data processing;

b. erasable and non-erasable memory modules for storage of data and software;

c. biometric scanner device for input of biometrics data;

d. data entry means for entering data;

e. digital communication port; and

f. means for prevention of electronic eavesdropping.

8. The apparatus of claim 7 wherein the computing modules are connected in a manner to prevent monitoring of communications between said computing modules.

9. The apparatus of claim 7 wherein the hardware component further comprises display means for display of data.

10. The apparatus of claim 7 wherein the hardware component further comprises RF shielding .

11. The apparatus of claim 4 wherein the hardware component further comprises a wireless communications means.

12. The apparatus of claim 7 wherein the biometric input means is secured from physical tampering.

13. The apparatus of claim 12 further comprising means for detection of physical penetration of the biometric input means.

14. The apparatus of claim 13 further comprising means for electronic self destruction whereby software and data stored within the memory module are erased.

15. The apparatus of claim 13 further comprising means for physical self destruction whereby the computing modules and memory modules are destroyed.

16. The apparatus of claim 4 wherein the hardware component further comprises means for reading magnetic strip cards.

17. The apparatus of claim 4 wherein the hardware component further comprises means for reading a smart card.
18. The apparatus of claim 4 wherein the software component resides in a computing module and further comprises;
    a. electronically erasable memory module wherein at least one command interface module, a first set of software and associated data specifically configured for the intended use of the biometric input device and data are stored; and
    b. non-erasable memory module wherein a second set of software and associated data are stored.
19. The apparatus of claim 18 said software component further comprising means for encryption of data from plaintext to ciphertext.
20. The apparatus of claim 18 said software component further comprising means to detect alteration of data further comprising;
    a. a secret key; and
    b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
21. The apparatus of claim 18 wherein the first set of software and associated data further comprising:
    a. biometric encoding algorithm; and
    b. encryption code.
22. The apparatus of claim 18 wherein the second set of software and associated data further comprising:
    a. an operating system; and
    b. at least one device driver.
23. The apparatus of claim 4 wherein said terminal is any electronic device and which issues commands to and receives results from the biometric input means.
24. The apparatus of claim 23 wherein said terminal is selected from the group of facsimile machines, telephones, television remote control, personal computers, credit/debit card processors, cash registers, automated teller machines, wireless personal computers
25. The apparatus of claim 4 wherein said second interconnecting means is means for wireless communications.
26. The apparatus of claim 1 wherein said first interconnecting means is selected from the group X.25, ATM network, Telephone network, Internet network, cable television network, cellular telephone network.

27. The apparatus of claim 1 wherein the comparison means further comprises means for encryption and decryption of data.
28. The apparatus of claim 1 wherein comparison means further comprises means for identifying the biometric input device.
29. The apparatus of claim 1 wherein the computer system further comprises:
    a. at least one independent computer network system; and
    b. third interconnecting means for interconnecting said computer system with said counter party computer system.
30. The apparatus of claim 29 wherein the third interconnecting means comprises an X.25 network.
31. The apparatus of claim 1 wherein the execution means comprises at least one database for storage and retrieval of data.
32. The apparatus of claim 31 wherein the data base further comprises an individual biometric data base.
33. The apparatus of claim 31 wherein the data base further comprises a prior fraud check data base.
34. The apparatus of claim 31 wherein the data base further comprises an electronic document data base.
35. The apparatus of claim 31 wherein the data base further comprises an electronic signature data base.
36. The apparatus of claim 1 wherein said output means is selected from the group of an X.25 network, ATM network, Telephone network, Internet network, cable television network.
37. The apparatus of claim 1 wherein said private code is generated by the computer.
38. A method for voluntary and tokenless identification of individuals, and authentication of the identification, said method comprising the steps of:
    a. registration step wherein at least one biometric sample, personal identification code, and private code from an individual is gathered and stored;
    b. bid step wherein at least one biometric sample and personal identification code from an individual is gathered;
    c. comparison step wherein the biometric sample and personal identification code gathered during the bid step is compared with the biometric sample and personal identification code gathered and stored during the registration step, for producing either a successful or failed identification result;

d. execution step wherein a command is processed and executed to produce a determination;

e. output step wherein said identification result or determination is externalized and displayed; and

f. presentation step wherein on successful identification of the individual, the private code is presented to the individual being identified.

39. The method of claim 38 wherein both the registration and bid steps further comprise a biometric sample check step wherein the quality of the biometric sample is verified.

40. The method of claim 38 wherein the registration step further comprises a personal identification code and biometric sample duplication check step wherein the biometrics and personal identification code gathered during the registration step is checked against all previously registered biometrics currently associated with the identical personal identification code.

41. The method of claim 38 wherein the registration step further comprises an ancillary data input step wherein ancillary data is collected.

42. The method of claim 41 wherein the ancillary data further comprises name and address of the individual.

43. The method of claim 41 wherein the ancillary data further comprises a title of an individual.

44. The method of claim 43 wherein the ancillary data input step further comprises a title index assignment step wherein each title of the individual is assigned a code.

45. The method of claim 41 wherein the ancillary data further comprises a financial asset account number.

46. The method of claim 45 wherein the ancillary data input step further comprises an account index assignment step wherein each financial asset account number is assigned an index code.

47. The method of claim 38 wherein the registration step further comprises a prior fraud check step wherein the biometric sample gathered during registration is compared to a subset of previously registered biometric samples.

48. The method of claim 38 wherein the registration step further comprises an emergency mechanism setup step.

49. The method of claim 48 further comprising an emergency account index assignment step wherein an account index is labeled as an emergency account where in the event the account is accessed appropriate authorities are notified of the emergency.

50. The method of claim 49 further comprising a false screen display setup step wherein there is assignment of false screen data.

51. The method of claim 49 wherein access to various financial asset accounts is limited.
52. The method of claim 38 wherein the registration step further comprises a modification step wherein any previously entered ancillary data can be modified or deleted.
53. The method of claim 38 wherein both the registration and bid steps further comprise a data sealing step to provide the ability to detect alteration of the data further comprising;
    a. a secret key; and
    b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
54. The method of claim 38, wherein the registration and bid steps further comprise an encryption step to convert the data from plaintext to ciphertext.
55. The method of claim 38 wherein the bid or registration steps further comprise a transmission step wherein the data is transmitted.
56. The method of claim 38 wherein the bid or registration steps is further provided with a unique transmission code having a unique hardware identification code and incrementing sequence number which increases by one for each transmission.
57. The method of claim 38 wherein the registration step further comprises choosing a language for communication in a set language step.
58. The method of claim 38 wherein the bid step further comprises choosing a title in a set title number step.
59. The method of claim 38 wherein the bid step further comprises choosing an account number in a set account number step.
60. The method of claim 38 wherein the bid step further comprises validating an amount in a validate amount step.
61. The method of claim 38 wherein the bid step further comprises entering an amount in an enter amount step.
62. The method of claim 38 wherein the bid step further comprises validating a document in a validate document step.
63. The method of claim 38 wherein the bid step further comprises appending ancillary data in an assign register step.
64. The method of claim 63 the ancillary data further comprising a counter party identification code.
65. The method of claim 38 wherein the bid or registration step further comprise aborting or canceling said step in a reset step.
66. The method of claim 38 wherein the bid step further comprises transmission of data in a transmission step.

67. The method of claim 38 wherein the bid step further comprises choosing a language for communication in a set language step.
68. The method of claim 38 wherein the comparison step further comprises use of the unique transmission codes to detect repeat transmissions.
69. The method of claim 38 wherein the comparison step further comprises a counter party identification step using the counter party identification and unique transmission codes.
70. The method of claim 38 wherein the comparison step comprises matching the individual's personal identification code and biometric gathered during the bid step, with the personal identification code and biometric gathered during the registration step for positive identification of the individual.
71. The method of claim 70 wherein if there is no match of the personal identification code and biometric gathered during the registration step and the personal identification code and biometric gathered during the bid step, there is no recognition of the individual.
72. The method of claim 38 wherein the execution step further comprises a debit/credit transaction step.
73. The method of claim 72 wherein the debit/credit transaction step further comprises an address collection step.
74. The method of claim 38 wherein the execution step further comprises an archiving step and a tracking code assignment step for archival of data.
75. The method of claim 74 wherein the data is sent through a message digest encoding algorithm step to produce an electronically signatured document.
76. The method of claim 38 wherein the execution step further comprises the retrieval of archived data using said tracking code.
77. The method of claim 38 wherein the execution step further comprises a modification step wherein the title index code, account numbers and account index codes are added, deleted or modified.
78. The method of claim 38 wherein the execution step further comprises an account number retrieval step where the account index code is used to retrieve an account number.
79. The method of claim 38 wherein the execution step further comprises an emergency activation step.
80. The method of claim 79 wherein the emergency activation step further comprises recognition of the emergency code and identifying the entire transaction as an emergency and notification of authorities.

81. The method of claim 79 wherein the execution step further comprises a false display step wherein previously designated, false accounts or false limitations on accounts are accessible.

82. The method of claim 38 wherein the output step further comprises an identification result notification step.

83. The method of claim 38 wherein the output step further comprises a determination notification step.

84. The method of claim 38 wherein the output step further comprises an emergency code step wherein authorities are notified.

85. The method of claim 38 wherein the output step further comprises display of false screens.

86. The method of claim 38 wherein the presentation step further comprises encryption, externalization, and decryption of the private code.

87. A method for rapid search of at least one first previously stored biometric sample from a first individual, using a personal identification code-basket that is capable of containing at least one algorithmically unique second biometric sample from at least one second individual, and which is identified by said personal identification code-basket, comprising:

a. a storage step further comprising;

i. selection of a personal identification code by said first individual;

ii. entering a biometric sample from said first individual;

iii. locating the personal identification code-basket identified by the personal identification code selected by said first individual;

iv. comparison of the biometric sample taken from said first individual, with any previously stored biometric samples in said selected personal identification code-basket, to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; and

v. storage of the entered biometric sample from said first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample from said at least one second individual; and

b. a bid step further comprising;

i. entering said selected personal identification code by said first individual; and

ii. entering a biometric sample by said first individual; and

c. a comparison step further comprising;

i. finding the personal identification code-basket that is identified by said personal identification code entered by said first individual; and

ii. comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result.

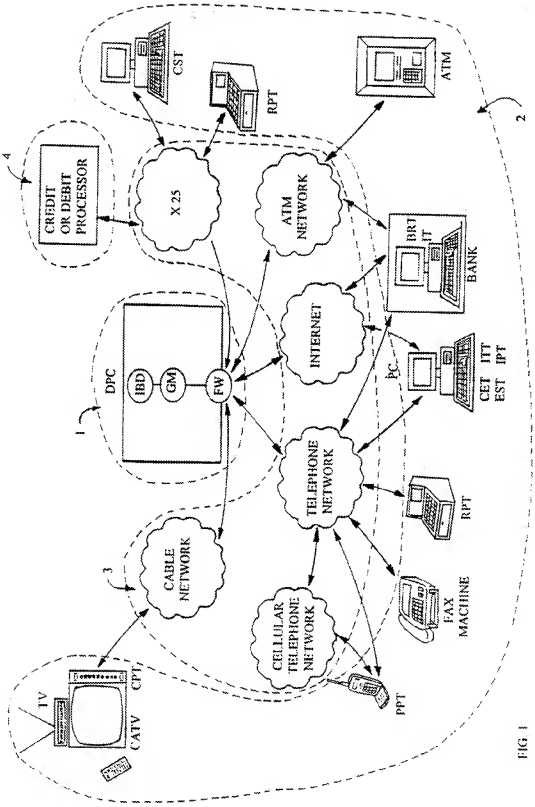
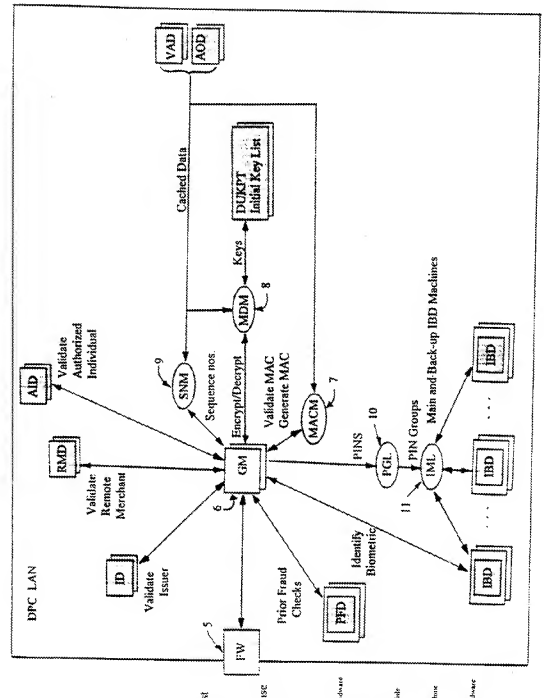

CST
RPT
ATM
4
CREDIT OR DEBIT PROCESSOR
X 25
ATM NETWORK
BRT IT BANK
DPC
IBD
GM
FW
INTERNET
PC
CET ITT EST IPT
1
TELEPHONE NETWORK
RPT
3
CABLE NETWORK
FAX MACHINE
CELLULAR TELEPHONE NETWORK
PPT
TV
CATV
CPT
2

FIG 1

FIG 2


DPC LAN
AID
Validate Authorized Individual
RMD
Validate Remote Merchant
ID
Validate Issuer
FW
5
6
GM
PFD
Prior Fraud Checks
Identify Biometric
9
SNM
Sequence nos.
Encrypt/Decrypt
MDM
8
Keys
DUKPT Initial Key List
Cached Data
VAD
AOD
Validate MAC
Generate MAC
MACM
7
PINS
10
PGL
11
PIN Groups
Main and Back-up IBD Machines
IML
IBD
IBD
IBD
Request Packet
Response Packet
KEY
= Computer Hardware
= Database
= Software Module
Dedicated Database Machine
Mirrored Computer Hardware
Mirrored Database

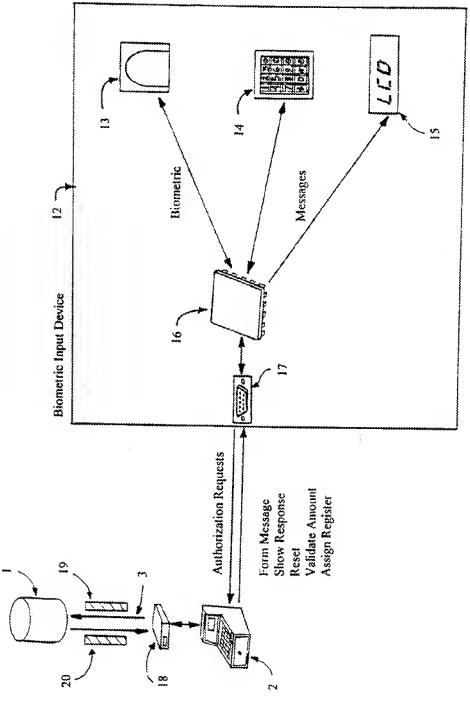

Biometric Input Device
12
13
14
15
LCD
Biometric
Messages
16
17
Authorization Requests
Form Message
Show Response
Reset
Validate Amount
Assign Register
1
19
3
20
18
2

FIG 3

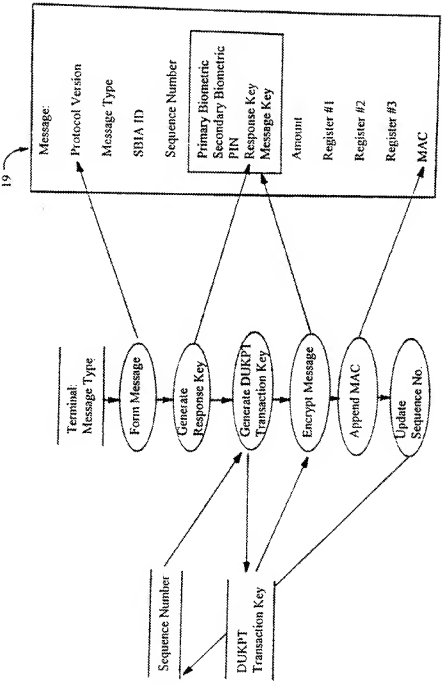

19
Message:
Protocol Version
Message Type
SHA ID
Sequence Number
Primary Biometric
Secondary Biometric
PIN
Response Key
Message Key
Amount
Register #1
Register #2
Register #3
MAC
Terminal Message Type
Form Message
Generate Response Key
Generate DUKPT Transaction Key
Encrypt Message
Append MAC
Update Sequence No.
Sequence Number
DUKPT Transaction Key

FIG. 4

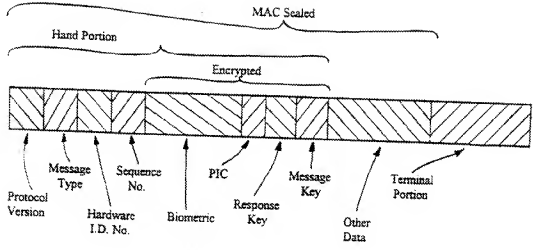

MAC Sealed
Hand Portion
Encrypted
Protocol Version
Message Type
Hardware I.D. No.
Sequence No.
Biometric
PIC
Response Key
Message Key
Other Data
Terminal Portion

FIG. 5

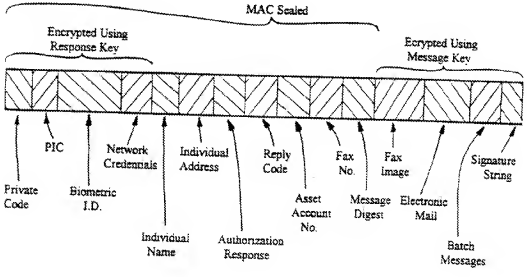

MAC Sealed
Encrypted Using Response Key
Ecrypted Using Message Key
Private Code
PIC
Biometric I.D.
Network Credennals
Individual Name
Individual Address
Authorization Response
Reply Code
Asset Account No.
Fax No.
Message Digest
Fax Image
Electronic Mail
Batch Messages
Signature String

FIG. 6

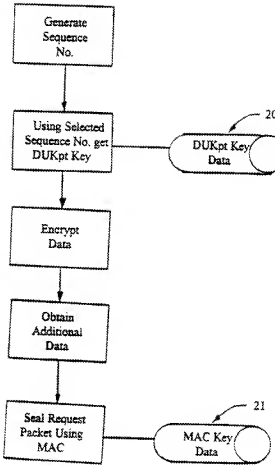

Generate Sequence No.
Using Selected Sequence No. get DUKpt Key
20
DUKpt Key Data
Encrypt Data
Obtain Additional Data
Seal Request Packet Using MAC
21
MAC Key Data

FIG. 7

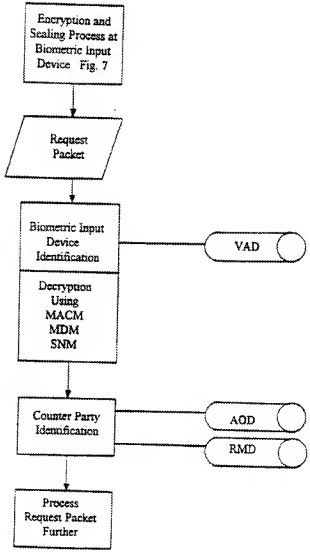

Encryption and Sealing Process at Biometric Input Device Fig. 7
Request Packet
Biometric Input Device Identification
VAD
Decryption Using MACM MDM SNM
Counter Party Identification
AOD
RMD
Process Request Packet Further

FIG. 8

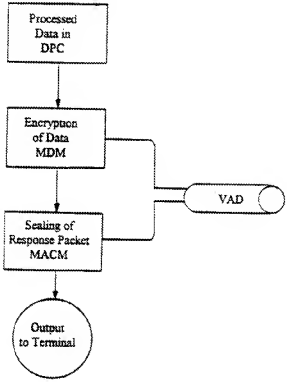

Processed Data in DPC
Encryption of Data MDM
VAD
Sealing of Response Packet MACM
Output to Terminal

FIG. 9

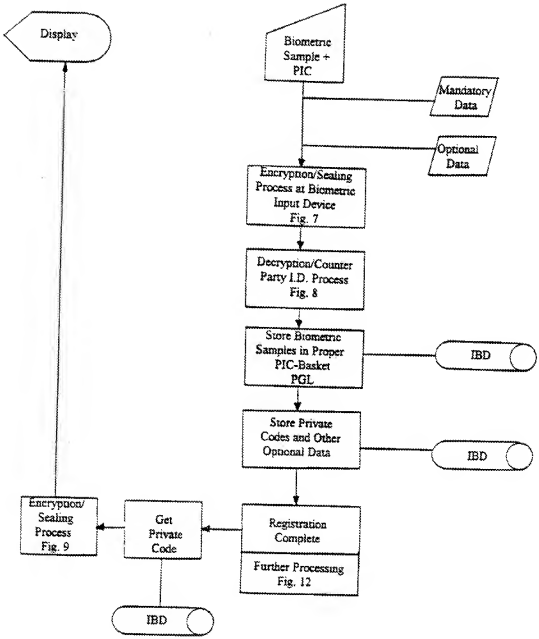

Display
Biometric Sample + PIC
Mandatory Data
Optional Data
Encryption/Sealing Process at Biometric Input Device Fig. 7
Decryption/Counter Party I.D. Process Fig. 8
Store Biometric Samples in Proper PIC-Basket PGL
IBD
Store Private Codes and Other Optional Data
IBD
Encryption/ Sealing Process Fig. 9
Get Private Code
Registration Complete
Further Processing Fig. 12
IBD

FIG. 10

PATENT

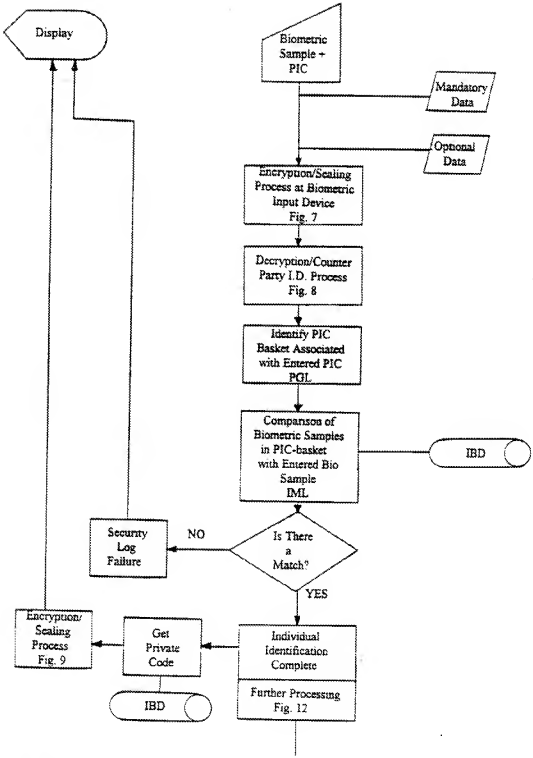


FIG. 11

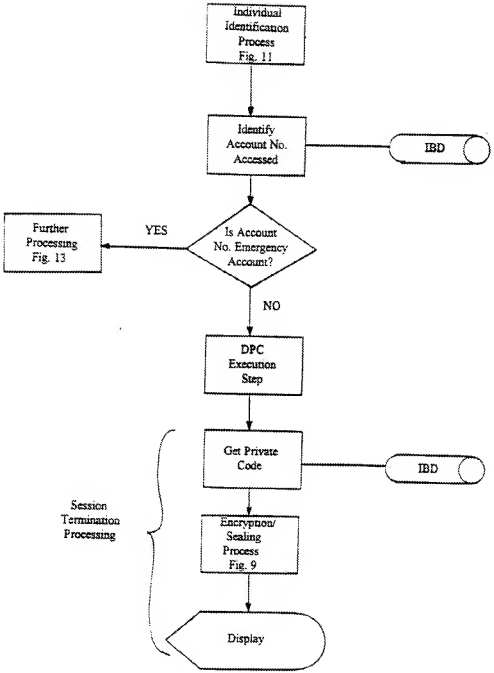

Individual Identification Process Fig. 11
Identify Account No. Accessed
IBD
Is Account No. Emergency Account?
YES
Further Processing Fig. 13
NO
DPC Execution Step
Get Private Code
IBD
Session Termination Processing
Encryption/ Sealing Process Fig. 9
Display

FIG. 12

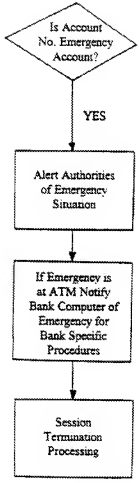

Is Account No. Emergency Account?
YES
Alert Authorities of Emergency Situation
If Emergency is at ATM Notify Bank Computer of Emergency for Bank Specific Procedures
Session Termination Processing

FIG. 13

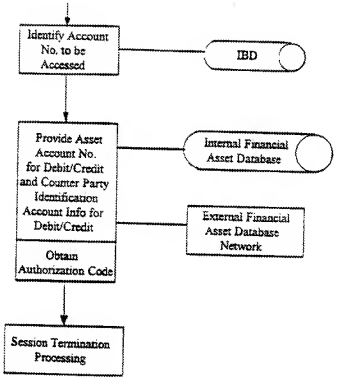

Identify Account No. to be Accessed
IBD
Provide Asset Account No. for Debit/Credit and Counter Party Identification Account Info for Debit/Credit
Internal Financial Asset Database
External Financial Asset Database Network
Obtain Authorization Code
Session Termination Processing

FIG. 14

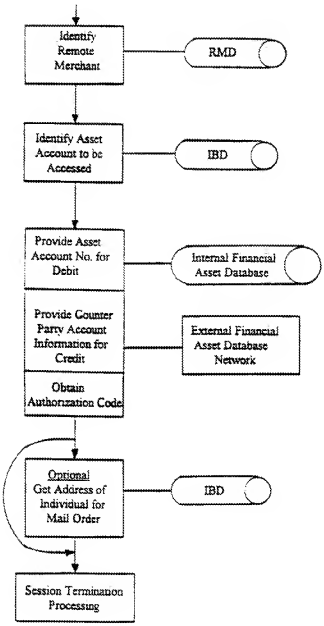

Identify Remote Merchant
RMD
Identify Asset Account to be Accessed
IBD
Provide Asset Account No. for Debit
Internal Financial Asset Database
Provide Counter Party Account Information for Credit
External Financial Asset Database Network
Obtain Authorization Code
Optional Get Address of Individual for Mail Order
IBD
Session Termination Processing

FIG. 15

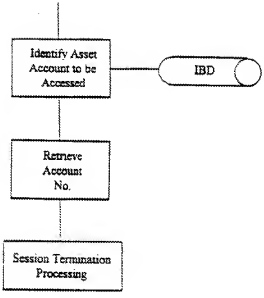

Identify Asset Account to be Accessed
IBD
Retrieve Account No.
Session Termination Processing

FIG. 16

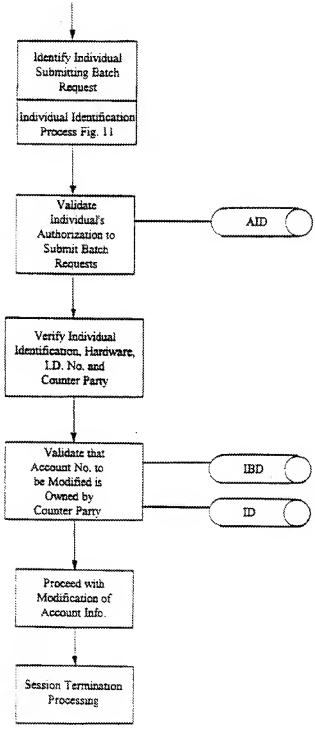

Identify Individual Submitting Batch Request
Individual Identification Process Fig. 11
Validate Individual's Authorization to Submit Batch Requests
AID
Verify Individual Identification, Hardware, I.D. No. and Counter Party
Validate that Account No. to be Modified is Owned by Counter Party
IBD
ID
Proceed with Modification of Account Info.
Session Termination Processing

FIG. 17

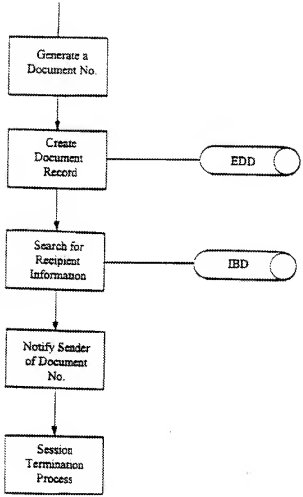

Generate a Document No.
Create Document Record
EDD
Search for Recipient Information
IBD
Notify Sender of Document No.
Session Termination Process

FIG. 18

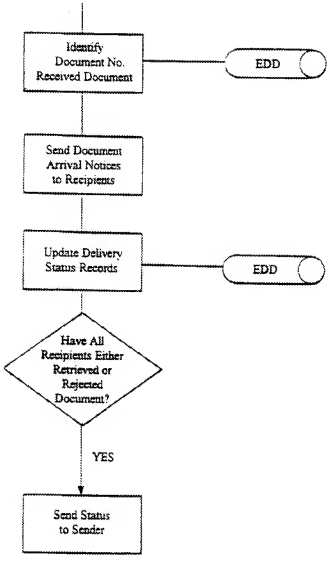

Identify Document No. Received Document
EDD
Send Document Arrival Notices to Recipients
Update Delivery Status Records
EDD
Have All Recipients Either Retrieved or Rejected Document?
YES
Send Status to Sender

FIG. 19

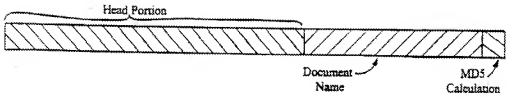


FIG. 20A

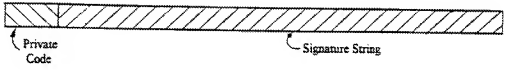


FIG. 20B

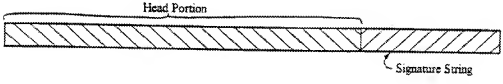


FIG. 20C

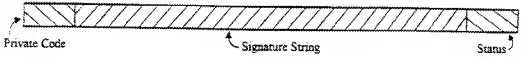


FIG. 20D

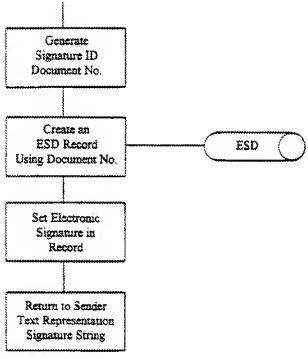

Generate Signature ID Document No.
Create an ESD Record Using Document No.
ESD
Set Electronic Signature in Record
Return to Sender Text Representation Signature String

FIG. 21

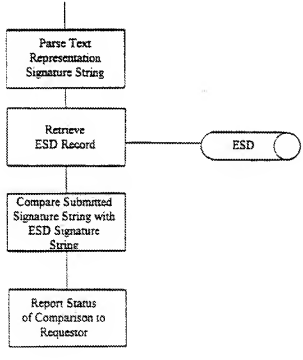

Parse Text Representation Signature String
Retrieve ESD Record
ESD
Compare Submitted Signature String with ESD Signature String
Report Status of Comparison to Requestor

FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 9/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,229,764 (MATCHETT ET AL) 20 July 1993, see abstract, figure 1, column 1, lines 6-59, column 8, lines 19-25.	1-87
Y	US, A, 5,191,611 (LANG) 02 March 1993, column 16, line 27.	1-87

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 03 JULY 1996	Date of mailing of the international search report 26 AUG 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LEO BOUDREAU Telephone No. (703) 308-7595

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115